NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

USING OPERATIONAL RISK MANAGEMENT (ORM) TO IMPROVE COMPUTER NETWORK DEFENSE (CND) PERFORMANCE IN THE DEPARTMENT OF THE NAVY (DON)

by

Ernest D. Hernandez

March 2001

Thesis Co-Advisors: Rex Buddenberg
Daniel Warren

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2001	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Using Operational Risk Management (ORM) to improve Computer Network Defense (CND) performance in the Department of the Navy (DON)	**5. FUNDING NUMBERS**
6. AUTHOR(S) Hernandez, Ernest David	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	**12b. DISTRIBUTION CODE**

ABSTRACT ***(maximum 200 words)***

Operational Risk Management (ORM) has been credited with reducing the Navy's mishap rate to all time lows, especially in Naval Aviation. Through the use of a five-step process, ORM has been able to change the decision makers' paradigm of day-to-day operations in naval fleet units, making safety the paramount factor that would allow fleet commanding officers to conserve their assets, yet meet the requirement to train in high-risk environments. ORM is a process that mitigates the risk associated with the high-risk environment that naval fleet units operate in. Not unlike naval fleet units, our computer networks operate in a high-risk environment-the Internet. Crackers are able to penetrate what were thought to be secure networks, and copy, modify, disrupt or destroy valuable information. The risk posed to the Navy's computer network systems is very great. Given the Navy's adoption of "Network-Centric Warfare" and the Navy-Marine Corps Intranet (NMCI), the hazards faced by the possible compromise of these computer network systems are as great as any a fleet unit would encounter in its normal operating environment. The objective of this thesis is to translate ORM practices into Information Assurance Risk Management (IARM) practices, and demonstrate IARM's utility in identifying, quantifying, and mitigating the security risks associated with computer networks.

14. SUBJECT TERMS Computer Network Defense (CND), Operational Risk Management (ORM), Critical Infrastructure Assurance, Information Assurance Risk Management (IARM), and Information Assurance (IA).	**15. NUMBER OF PAGES** 154
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFI- CATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

USING OPERATIONAL RISK MANAGEMENT (ORM) TO IMPROVE COMPUTER NETWORK DEFENSE (CND) PERFORMANCE IN THE DEPARTMENT OF THE NAVY (DON)

Ernest David Hernandez
Lieutenant Commander, United States Navy
B.S., United States Naval Academy, 1985

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2001

Author: Ernest D. Hernandez
Ernest David Hernandez

Approved by:
Rex Buddenberg, Thesis Co-Advisor

Daniel Warren, Thesis Co-Advisor

Dan C Boger
Dan C. Boger, Chairman
Information Systems Academic Group

ABSTRACT

Operational Risk Management (ORM) has been credited with reducing the Navy's mishap rate to all time lows, especially in Naval Aviation. Through the use of a five-step process, ORM has been able to change the decision makers' paradigm of day-to-day operations in naval fleet units, making safety the paramount factor that would allow fleet commanding officers to conserve their assets, yet meet the requirement to train in high-risk environments. ORM is a process that mitigates the risk associated with the high-risk environment that naval fleet units operate in.

Not unlike naval fleet units, our computer networks operate in a high-risk environment-the Internet. Crackers are able to penetrate what were thought to be secure networks, and copy, modify, disrupt or destroy valuable information. The risk posed to the Navy's computer network systems is very great. Given the Navy's adoption of "Network-Centric Warfare" and the Navy-Marine Corps Intranet (NMCI), the hazards faced by the possible compromise of these computer network systems are as great as any a fleet unit would encounter in its normal operating environment.

The objective of this thesis is to translate ORM practices into Information Assurance Risk Management (IARM) practices, and demonstrate IARM's utility in identifying, quantifying, and mitigating the security risks associated with computer networks.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

3DES	Triple-Data Encryption Standard
AH	Authentication Header
BDC	Back-up Domain Controller
CA	Certificate Authority
CBC	Cipher Block Chaining
CHAP	Challenge Handshake Authentication Protocol
CRL	Certificate Revocation List
DDOS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server or Services
DoD	United States Department of Defense
DON	Department of the Navy
DSL	Digital Subscribers Line
EAP	Extensible Authentication Protocol
ECB	Electronic Code-book Mode
ESP	Encapsulated Security Protocol
FY	Fiscal Year
GAO	Government Accounting Office
GRE	Genetic Routing Encapsulation
HMAC	Hashed Message Authentication Code
IA	Information Assurance
IARM	Information Assurance Risk Management
ICV	Integrity Check Value
IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPCP	IP Control Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IO	Information Operations
IS	Information System
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
IT	Information Technology
KDC	Key Distribution Center
L2F	Layer 2 Forwarding protocol
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LCP	Link Control Protocol

LDAP	Lightweight Directory Access Protocol
LNS	L2TP Network Server
MAC	Message Authentication Code or Media Access Control
MD4	Message Digest 4
MD5	Message Digest 5
MIT	Massachusetts Institute of Technology
MPPE	Microsoft's Point-to-Point Encryption
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NAS	Network Access Server
NCP	Network Control Protocol
NIST	National Institute of Standards and Technology
NMCI	Navy and Marine Corps Intranet
NOC	Network Operations Center
NPS	Naval Postgraduate School
NSA	National Security Agency
NSC	Naval Safety Center
ORM	Operational Risk Management
OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PDC	Primary Domain Controller
PFS	Perfect Forward Security
PGP	Pretty Good Privacy
PHA	Preliminary Hazard Assessment
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Server or Services
RSA	Rivest, Shamir, and Adleman
SA	Security Association
SAD	Security Association Database
SHA-1	Secure Hash Algorithm 1
SPAWAR	Space and Naval Warfare Systems Command
SPD	Security Policy Database
SPI	Security Parameter Index
SRM	Security Risk Management
SSH	Secure Shell
TCP	Transmission Control Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web
XAUTH	Extended Authentication

ACKNOWLEDGEMENT

The author would like to acknowledge the opportunities afforded the author from the United States Navy. Not only was the author allowed to fly the most sophisticated aircraft in the world and pilot the largest military vessels to transverse the world's oceans, the Navy has also allowed the author to attend the Naval Postgraduate School and continue to expand his horizons both professionally and intellectually.

The author also wants to recognize certain people, for without whom, this thesis would not be what it is today. First and foremost is his loving wife, a person of boundless patience and energy, for her incredible abilities as a mother, Naval Officer, and fellow student here at the Naval Postgraduate School. To my two children, David and Rachel, may our endeavors today be worthy enough to build a safe future for you tomorrow.

Thanks also goes out to Rex Buddenberg and Daniel Warren for advising me on my thesis, and for asking the tough questions and supporting my ideas; to the Network Operations team here at NPS, and specifically to Lonna Sherwin and Bob Gentry for allowing me the use of the new research lab, and Carol Rojas for the use of the equipment; to Jay Matos for his excellent work on VPN vulnerabilities assessment; and to Scott Cote, a fellow student and close friend, for all his help and technical assistance, as well as the talks I enjoyed about everything and anything. Good luck in your new life as a civilian!

And to John F. Kennedy for his inspiring words:

"Man is still the most extraordinary computer of all."

John F. Kennedy

I. INTRODUCTION

A. BACKGROUND

The Navy Marine Corps Intranet mission statement, "To enable the sharing of information worldwide with those who need it, when they need it, and to enhance enterprise-wide work, training, and quality of life for every Marine, Sailor, and DON Civilian," typifies the Department of the Navy's (DON) push towards leveraging the capabilities of information technology and the Internet to aid in making the DON a more efficient and effective organization. In embarking on the NMCI, the DON has acknowledged that the quick and unencumbered exchange of information is an extremely important commodity in bringing the DON into the 21st century. The DON has also adopted as its new tactical philosophy "Network-Centric Warfare." This new philosophy builds on the premise of gaining "knowledge superiority" using high speed and high capacity sensors and networks as a tactical advantage over any potential adversaries. This enterprise-wide access of information exposes DON networks to much of the same risks that are being faced today by commercial companies who use the Internet to conduct business to client and business-to-business transactions.

Two events that clearly illustrate the risks posed to DON and DOD computer network systems are the "Moonlight Maze" investigation and the DOD "Eligible Receiver" war game. As reported by the *Washington Times* on 16 April 1998, Eligible Receiver was a military exercise that demonstrated how vulnerable military and civilian networks are to attack by hackers (Gertz). An NSA "Red Team," posing as "make-believe hackers," used software freely available in the Internet to break into unclassified military computer networks in Hawaii, the headquarters of the U.S. Pacific Command, as well as in Washington, Chicago, St. Louis and parts of Colorado. The NSA Red Team clearly demonstrated their ability to disrupt the command and control capability in the Pacific theater. Also demonstrated were that attacks on the U.S. power grid were possible that could have succeeded in bringing it down. These attacks were possible because the Red Team was able to breach the Pentagon's unclassified global computer system (NIPRNET) using Internet service providers and dial-in connections that allowed them to go from network system to network system, enabling them to hide their true locations. Eligible Receiver was one of the motivating factors in getting the Clinton administration to create the Commission on Critical Infrastructure.

The Moonlight Maze investigation was initiated after it was discovered that a series of intrusions into government networks *appear* to have originated from Russia. In testimony before the Senate Judiciary Committee's subcommittee on technology, terrorism and government information, Michael Vitas, director of the National Infrastructure Protection Center, said the intrusions took large amounts of sensitive but unclassified (SBU) data, including defense technology research information (Johnston). Michael Vitas is further quoted:

> We know that several foreign nations are already developing information warfare doctrines, programs and capabilities. They see that they cannot defeat the United States in head-to-head military encounter and they believe that information operations are a way to strike at what they perceive as America's Achilles Heel: our reliance on information technology to control critical government and private sector systems.

Moonlight Maze illustrates that attacks on our computer networks may be as active a part of hostilities as the actual use of conventional weapons in future conflicts.

Eligible Receiver and Moonlight Maze illustrate what can happen when the risks to computer network systems are not properly managed. These risks go largely unchecked because of the ignorance towards information assurance in many organizations. The Department of Defense (DoD) is a prime example where the lack of knowledge about information assurance issues have led to little or no risk management to DoD computer networks. Mrs. Chey Cobb, a recently retired 20-year DoD employee, made some very pointed observations in this regard. Mrs. Cobb has worked in DoD firewall certification and anti-virus testing labs, has been involved with Web security since 1994, helped develop DoD and intelligence systems architectures, has served as a senior technical security advisor for the Intelligence Community and as a DoD security program manager. She cites in a presentation titled "Why Government Systems Fail at Security," that many key decision makers are ignorant and unaware of computer network security issues. She states that not enough money is spent on system administrator training and that many users have poor security habits, like using easy passwords or keeping the same password over an extended period of time. She bolsters her argument by citing a 1998 General Accounting Office (GAO) survey (www.gao.gov/AIndexFY98/category/Inform.htm) of security officers:

- 66% stated didn't have enough time or training to do their jobs.

-53% stated that security was an ancillary duty.

-43% were totally unaware of what they should be doing.

-57% had no security training.

Mrs. Cobb further states that IT support personnel and security officers rely too much on technical tools like firewalls and intrusion detection systems (IDS) as the "cure" for computer network security.

The civilian computer-security community has long since realized security hardware and software tools are not the only answer. Alan Paller, director of research for the SANS (System Administration and Network Security) Institute in the March 2000 issue of *Government Computer News*:

> The dirty little secret of computer security is that tools don't solve the problems. The tools provide a false sense of security. The reality of what solves the problem is training IT support personnel to systematically protect their systems. Because it doesn't matter what kind of hardware and software you use, you cannot protect the system if they don't do it right.

The above observations illustrate the need for a more disciplined and methodic approach to computer network security that is centered on *people*.

A proven, people-focused method to control risks that can be adapted to risks associated with network security originated with the United States Army and is called Operational Risk Management (ORM). ORM has been credited with reducing the Navy's mishap rate to all time lows, especially in Naval Aviation. Through the use of a five-step process, ORM has been able to change the decision makers' paradigm of day-to-day operations in naval fleet units. Before the use of ORM, unit Commanding Officers measured success by meeting mission goals. If mishaps occurred, it was attributed to the cost of doing business given the high-risk environment that naval fleet units operated in. As the Navy and the military contracted after the break up of the Soviet Union, they were forced to conserve their assets due to the high cost of replacing resources lost through mishaps and reduced funding availability. Concurrently, the high cost of new weapon systems and the considerable investment required in training personnel required that the Navy change its priorities in the way it conducted its day-to-day operations. Safety was deemed to be the paramount factor that would allow fleet commanding officers to conserve their assets, yet meet the requirement to train in high-risk environments. The ORM process changed commanding officers' priorities. Now safety was deemed to be the number one priority in training and conducting day-to-day operations. ORM was a process that mitigated the risk associated with the high-risk environment that naval fleet units operate in and facilitated a paradigm shift that put safety at the top of decision makers' priorities.

Not unlike naval fleet units, our computer networks operate in a high-risk environment-the Internet. Crackers are able to penetrate what were thought to be secure networks and copy, modify, disrupt or destroy valuable information. A computer virus can cause damage to networks through the deletion of data or denial of service. Distributed denials of service attacks on target systems through various remotely compromised systems are common occurrences. A proliferation of cracker tools is available for easy download and use has produced the "script kiddies" widely known today. The risk posed to the Navy's computer network systems is very great and is exacerbated by user and decision maker ignorance of computer network security. Given the Navy's adoption of "Network-Centric Warfare" and the deployment of the Navy-Marine Corps Intranet (NMCI), the hazards faced by the possible compromise of these computer network systems are as great as any a fleet unit would encounter in its normal operating environment.

B. PURPOSE OF RESEARCH

The objective of this thesis is to translate ORM practices to Information Assurance Risk Management (IARM) practices, demonstrate IARM's utility in identifying, quantifying, and mitigating the security risks associated with computer networks for the Department of the Navy (DON). Finally, demonstrate that "network security" should be elevated to the same level of importance as "safety" in aviation.

Specific research questions the author sets out to answer are:

1. Can the ORM process be tailored/modified to fit the security risk associated with computers and networks?

2. Can an Information Assurance Risk Management (IARM) process be developed from ORM and be used to effectively improve the Computer Network Defense (CND) performance on DON network systems?

3. Can IARM be used to make effective information technology procurement decisions in regards to security criteria?

C. SCOPE, METHODOLOGY, LIMITS, ASSUMPTIONS

This thesis is limited in its scope. The scope will include: (1) a review of the ORM process, (2) an analysis of how ORM can be applied to computer networks, (3) the development of CRSM, (4) a demonstration of how IARM can improve CND and thus computer network security through out the fleet, and (5) a demonstration of how IARM can be applied to the procurement of new IT. Details of how IARM can be specifically applied to particular networks and IT systems are left to the organization to best suit their particular environment.

The research methodology used in writing this thesis included a combination of methods. Extensive literary research was first performed using the resources listed in the bibliography. Additional education on the subject was obtained from attending the SANS Network Security 2000 conference, Monterey, CA, October 2000. Previous to reporting to the Naval Postgraduate School, the author attended the six-week Aviation Safety Officer course, also here at NPS, from August to September 1996. During that course the principles of Operational Risk Management (ORM) were taught in a practical approach for application in the fleet. The author then applied ORM in an operational environment as the Safety Officer for an F-14 squadron from April 1997 to June 1998. During that period the squadron performed high-tempo operations from both shipboard and land environments. Hands on computer network experience was gained by working with the NPS Network Operations staff in understanding the current network architecture of the NPS intranet, and from creating a custom research lab that was a mock-up of the intranet. This mock-up was then subjected to the installation of different VPN technologies, including a TimeStep© 7520 gateway appliance. The author earned a Global Incident Analysis Center (GIAC) Security Essentials Certification (GSEC) from the SANS Institute in November 2000 and was certified as a Microsoft Systems Certified Engineer (MCSE) in December 2000.

There are certain assumptions the author made in writing this thesis. Though there will be an extensive review of key concepts, it is expected that the reader has a basic understanding of how networks function. This includes understanding the Internet Protocol (IP) and functions of basic network components such as routers and firewalls.

D. THESIS ORGANIZATION

The author has organized this thesis into four chapters. Chapters I is meant as an introduction to the concepts that will be covered in greater depth later in the thesis. Chapter II provides background information for those readers unfamiliar with

Operational Risk Management (ORM). Chapter III contains the heart of the thesis, discussing how Information Assurance Risk Management (IARM) can be developed from ORM, and how it can have a positive, qualitative impact on Computer Network Defense (CND). It is here that IARM will be developed and applied to CND and the development of IT systems. Chapter IV encompasses the author's recommendations on actually implementing Information Assurance Risk Management (IARM) in the DON. It also discusses conclusions and possible areas for further research.

II. OPERATIONAL RISK MANAGEMENT (ORM)

A. MOTIVATION BEHIND ORM

Navy units, especially those associated with carrier aviation, operate in some of the most hazardous operational environments known. Flying aircraft, both high-performance jets and helicopters, from ships is a very high-risk endeavor. An unwanted, but inevitable result has been many mishaps to equipment and personnel. Figure 1 shows the different programs that have been instituted in Naval Aviation in an attempt to reduce the mishap rate. The figure shows the trend for the mishap rate decreasing as a result of systematic changes applied to equipment and procedures designed to manage risk.

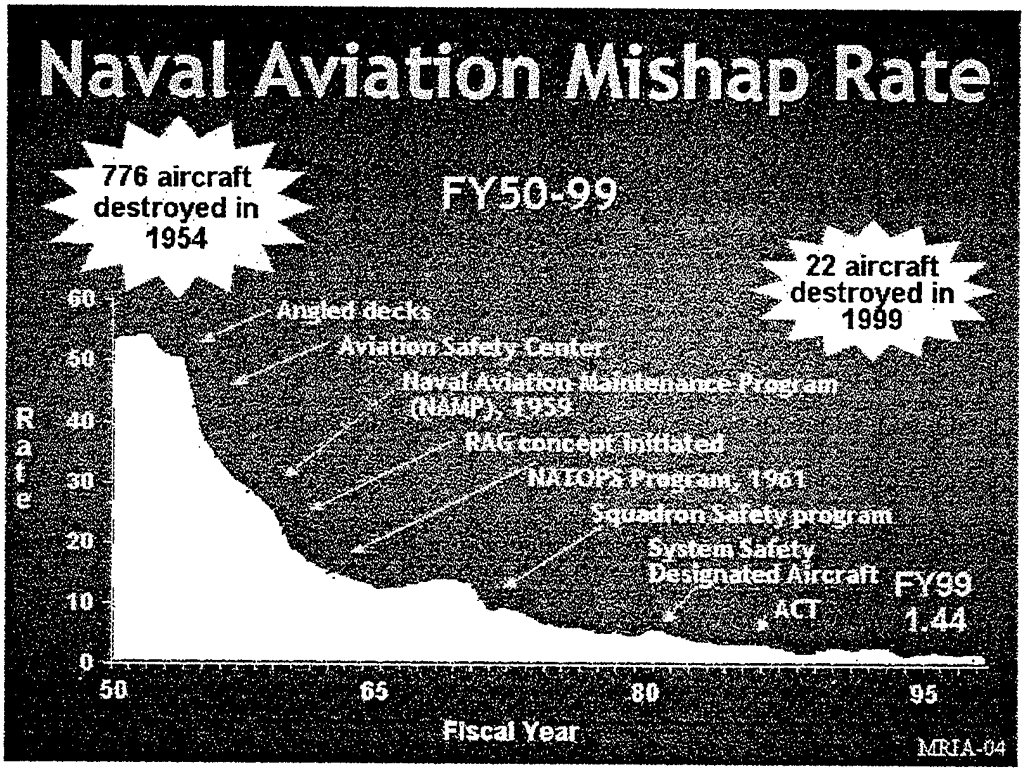


Figure 2-1. Naval Aviation Mishap Rate (From U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)

These programs, which were successful attempts of assessing risks and implementing controls, are viewed largely as reactive in nature because they corrected known deficiencies in equipment reliability and operating procedures *after* being identified in an operational environment. Though the beneficial result has been a decline in the mishap rate, it has leveled off. Conventional risk management of equipment reliability and standard operational procedures has been largely optimized. Though the benefits of this approach remain, we have reached a point of diminishing returns.

While the mishap rate did decline, the overall monetary costs associated with these mishaps did not. Due to the technical complexity of today's equipment, the cost of aircraft and personnel training has increased significantly, as has the cost associated with each mishap. From FY-95 to 99, aviation related mishaps have cost the Navy $3.3 billion. (Naval Safety Center) In the fiscal environment of the nineties, where the military was undergoing a significant downsizing, losses due to mishaps were viewed as having an adverse effect on readiness. The focus of risk management had to be re-orientated to those factors still causing mishaps - human error. Figure 2-2 depicts the annual frequency of mishaps with a monetary value of $10,000 or more attributable, at least in part, to human error, and those solely attributed to mechanical failures, between 1977 and 1992. The chart shows that while the mishaps attributed to mechanical error declined to about 1 in every 100,000 flight hours, those attributed to human error has not kept pace and only declined to about 7 in every 100,000 flight hours. (NSC) Furthermore, of all Navy and Marine Corps aviation mishaps from FY 90 to 96 that resulted in a fatality, or a

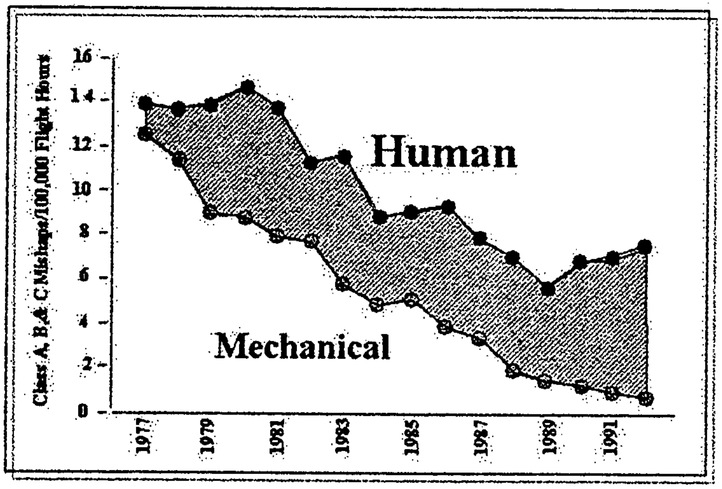


Figure 2-2. All Navy-Marine Corps Mishaps, CY 1977-92 (From U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)

monetary loss of $1 million or more, over 80% was determined to have human error as a causal factor. (NSC) The answer, as will be discussed below, to reducing the mishaps caused by human error was a new form of risk management – Operational Risk Management (ORM).

B. THE ORM PROCESS - INTRODUCTION

Operational Risk Management originated in the U.S. Army when it was adopted in the late 1980s as a process to improve safety among its ranks. In its most fundamental form, ORM does not aim to eliminate risk, but to manage risk so that the mission can be accomplished with the minimum amount of loss due to accidents. It is presented as a standardized tool to aid people working in a high-risk environment to *pro-actively* prevent mishaps. People make decisions based on what they perceive to be important to accomplishing their purpose in life. Through a five-step process, ORM seeks to change the way people perceive risk in their environment by providing the best baseline of knowledge and experience available in which to make informed decisions. ORM minimizes risks to acceptable levels by systematically applying controls to each risk that is not acceptable. It seeks to change cultural attitudes towards risk taking by making accident prevention the primary consideration when making decisions. Consequently, ORM is not just applicable to the high-risk environment of Naval Aviation, but to every environment where the risk of equipment loss or personal injury is present. The Navy's intention is to promote ORM as a process, even a way of life, not a program, and make it applicable to each individual's way of thinking.

C. ORM TERMS

The following are terms as applied to ORM in an operational environment. They are present here to facilitate a more in-depth discussion on the five-step ORM process later.

1. Hazard

A condition with the potential to cause personal injury or death, property damage, or mission degradation. Examples include enemy threats, security threats, inefficient use of assets, something, which can damage the organization's image and credibility, etc.

2. Risk

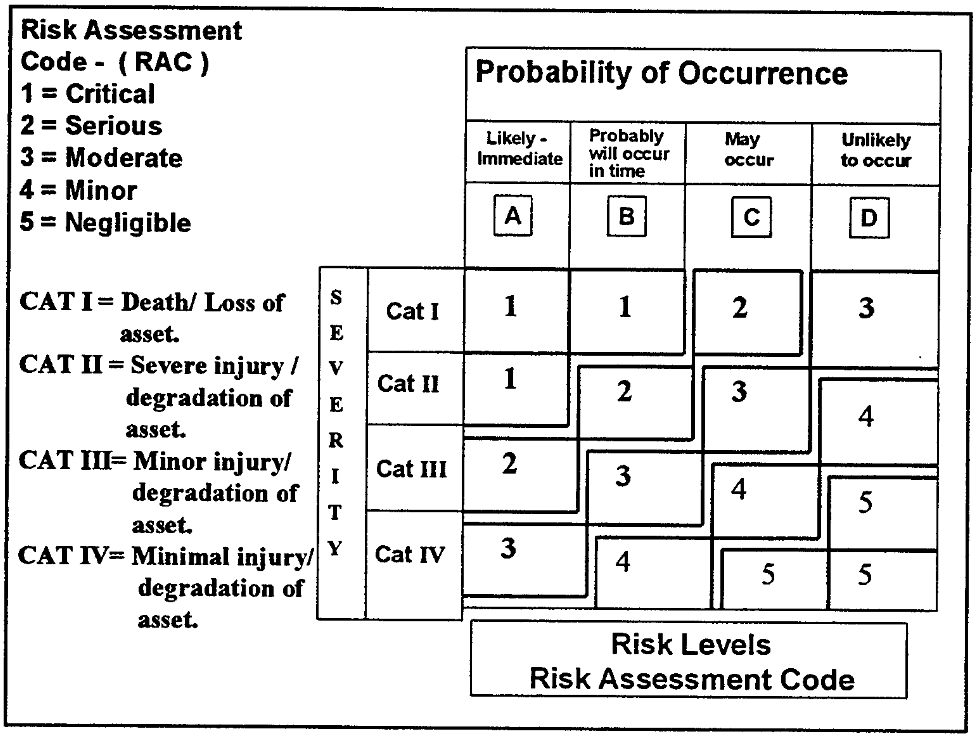
An expression of possible loss in terms of severity and probability.

3. Severity

The worst, credible consequence that can occur as a result of a hazard. It is the potential degree of loss. It is an expression of how serious the injury or illness, how much equipment damage, how much lost time, money, man-hours or credibility could be experienced as a result of the hazard.

4. Probability

The likelihood that a hazard will result in a mishap or loss, or cause a mission degradation. Based on factors such as location, exposure, personnel, experience and historical information.



Risk Assessment Code - (RAC)
1 = Critical
2 = Serious
3 = Moderate
4 = Minor
5 = Negligible

CAT I = Death/ Loss of asset.
CAT II = Severe injury / degradation of asset.
CAT III= Minor injury/ degradation of asset.
CAT IV= Minimal injury/ degradation of asset.

		Probability of Occurrence			
		Likely - Immediate A	Probably will occur in time B	May occur C	Unlikely to occur D
SEVERITY	Cat I	1	1	2	3
	Cat II	1	2	3	4
	Cat III	2	3	4	5
	Cat IV	3	4	5	5

Risk Levels
Risk Assessment Code

Figure 2-3. Risk Assessment Code Chart (From U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)

5. Risk Assessment

The process of detecting hazards and assessing the associated risk. It is the first two steps of the ORM process. The result is a risk assessment code (RAC) derived from the chart in figure 2-3.

6. Controls

A method for reducing risk for an identified hazard by lowering the probability of occurrence, decreasing potential severity, or both.

7. Operational Risk Management

The process of dealing with risk associated with military operations, which includes risk assessment, risk decision-making, and implementation of effective risk controls.

D. THE ORM PROCESS

The operational risk management process is a simple five-step process. It is a continuous process designed to detect, assess, and control risk while enhancing performance and maximizing capabilities. It was adapted from the concept of applying a standard, systematic approach to minimizing risk that was originally developed to improve safety in the development of weapons, aircraft, space vehicles, and nuclear power. The five steps are:

1. Identify Hazards

Identify potential causes of injury, damage or mission degradation. Specific actions include a mission/task analysis, listing hazards and listing causes for those hazards.

2. Assess Hazards

For each hazard identified, determine the associated risk in terms of severity and probability. Specific actions include assessing the exposure, severity and probability to the hazards listed in step 1.

3. Make Risk Decisions

Develop risk control options, and then decide if benefits outweigh risks. Seek further controls or guidance from superiors if necessary. Specific actions include identifying control options, determining the effects of those controls, prioritizing risk control measures, selecting risk controls and making risk decisions.

4. Implement Controls

Once the risk decisions are made, implement selected controls. Specific actions include making implementation of the above controls clear, establish accountability, and provide support.

5. Supervise

Follow-up to ensure controls are working and watch for changes. Specific actions include supervising the control implementation, monitoring for effectiveness, collecting feedback on the controls and monitoring for change. The summary of specific actions associated with each step of the ORM process is listed below in figure 2-4.

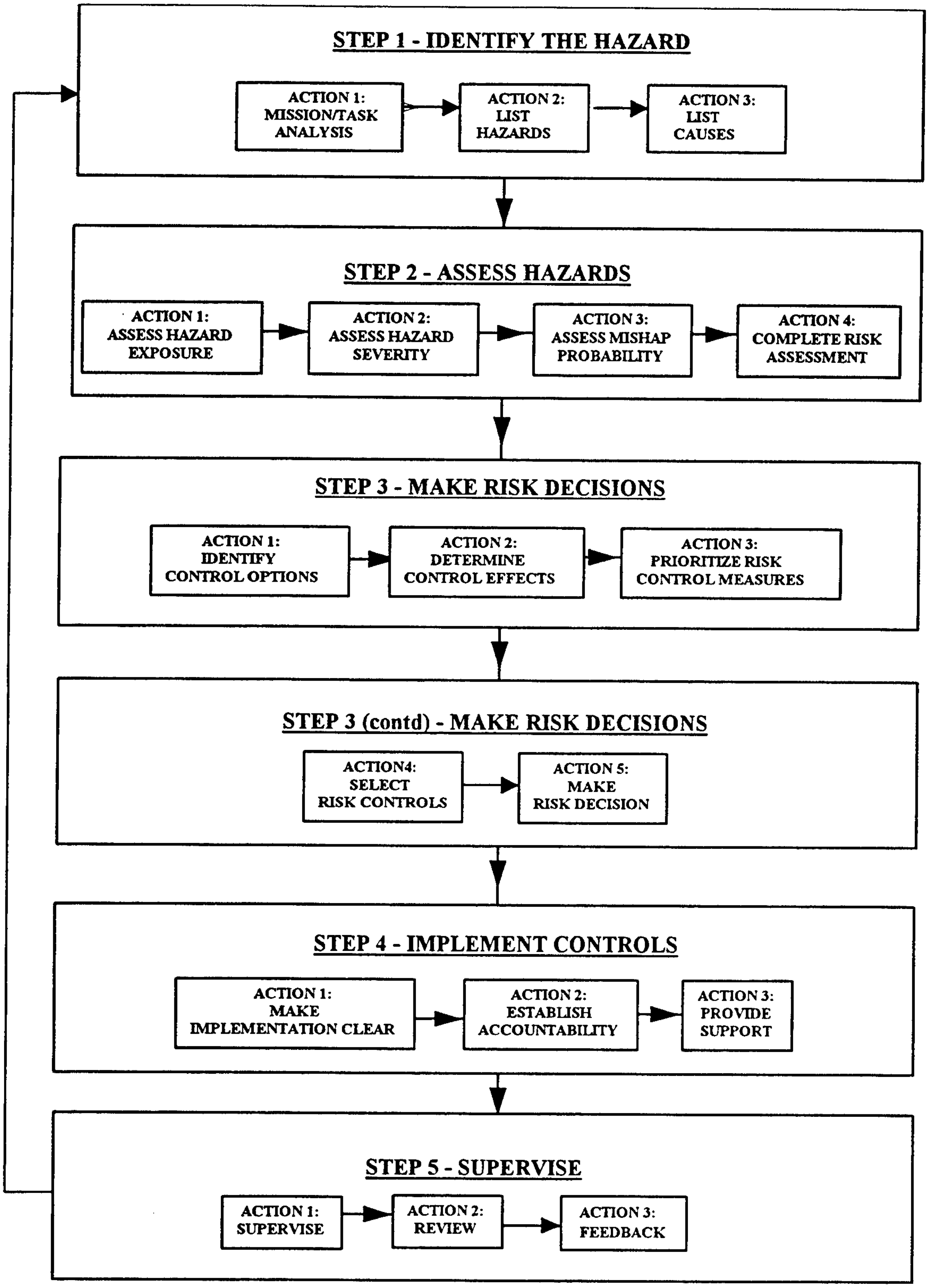

STEP 1 - IDENTIFY THE HAZARD
ACTION 1: MISSION/TASK ANALYSIS
ACTION 2: LIST HAZARDS
ACTION 3: LIST CAUSES
STEP 2 - ASSESS HAZARDS
ACTION 1: ASSESS HAZARD EXPOSURE
ACTION 2: ASSESS HAZARD SEVERITY
ACTION 3: ASSESS MISHAP PROBABILITY
ACTION 4: COMPLETE RISK ASSESSMENT
STEP 3 - MAKE RISK DECISIONS
ACTION 1: IDENTIFY CONTROL OPTIONS
ACTION 2: DETERMINE CONTROL EFFECTS
ACTION 3: PRIORITIZE RISK CONTROL MEASURES
STEP 3 (contd) - MAKE RISK DECISIONS
ACTION4: SELECT RISK CONTROLS
ACTION 5: MAKE RISK DECISION
STEP 4 - IMPLEMENT CONTROLS
ACTION 1: MAKE IMPLEMENTATION CLEAR
ACTION 2: ESTABLISH ACCOUNTABILITY
ACTION 3: PROVIDE SUPPORT
STEP 5 - SUPERVISE
ACTION 1: SUPERVISE
ACTION 2: REVIEW
ACTION 3: FEEDBACK

Figure 2-4. The Cyclic ORM Process (After U.S. Air Force ORM Process)

E. CAUSES OF RISK

A discussion of some of the factors that cause risk is useful. It facilitates a more thorough understanding of how hazards develop in our every day activities and how people using ORM to control risks associated with those hazards can be more effective in identifying them.

1. Change

In almost every environment, change is typically known as the "Mother" of all risk. The majority of people do not react favorably to change, especially when it's abrupt. Changes should alert us to new hazards and increased risk.

2. Resource Constraints

In the last decade, the military has had to operate under the motto of "doing more with less," stretching to the limits the resources it has available to perform its mission. An undesirable consequence is that it adds risk to one's environment due to the inability to answer the question, "how long can we keep stretching our resources?"

3. New Technology

Though new technology can improve reliability and reduce risk, particularly second-generation implementations, the gains are often offset by our human abilities to absorb all the new information it provides, or adapt to the new equipment.

4. Complexity

The more complex the problem, the more riskier. There are more ways for things to go wrong.

5. Stress

As pointed out above, human error has been cited in over 80% of aviation mishaps for FY-90 to 96. Stress significantly affects the abilities of humans to perform in risky environments.

6. Human Nature

It is our nature to make mistakes, mis-communicate, have personality conflicts, get fatigued, get complacent, and so on. Human nature must be taken into account for the inherent risks it introduces in our day-to-day activities.

7. Inexperience

Rapid personnel turn over significantly degrades our ability to build corporate knowledge at the organization level.

8. High Energy Levels

Nervous energy, excitement associated with new situations and perceived pressure to perform can all increase risk. A study of Naval Air Force Atlantic and Pacific Fleet accidents shows that 56% of the deployment mishaps from FY-91 to first quarter FY-96 occurred during the first two months of an extended deployment.

9. Societal Constraints

Society's standards and expectations drive public opinion, which has an important bearing on military budgets. Events that negatively affect an organization's image in the public eye can certainly present risk. The after math of the Vietnam War is a classic example.

10. Environmental Influences

The physical environment is always a significant consideration. The likelihood of natural disasters and extremes of weather always pose a risk to equipment and personnel.

11. Speed/Tempo of Operation

Risk can increase when the tempo for an organization is unusually high, or when it is unusually low, due to complacency.

F. THE FOUR ORM PRINCIPLES

These principles are indispensable to understanding how ORM improves the way people make decisions about risk. They govern all actions associated with risk management. These principles are applicable before, during, and after all tasks and operations.

1. Accept No Unnecessary Risk

Unnecessary risk comes without a commensurate return in terms of real benefits or available opportunities. All military missions, tasks and our daily routines involve risk. The most logical choices for accomplishing a mission or task are those that meet all mission/task requirements with the minimum acceptable risk. The corollary to this axiom is "accept necessary risk" required to successfully complete the mission or task.

2. Make Risk Decisions at the Appropriate Level

Making risk decisions at the appropriate level establishes clear accountability. Those accountable for the success or failure of the task must be included in the risk decision process. The appropriate level for risk decisions is the one that can allocate the resources to reduce the risk or eliminate the hazard and implement controls. Typically, the commander, leader, or individual responsible for executing the mission or task is:

a. Authorized to accept levels of risk typical of the planned operation/task (i.e., loss of mission effectiveness, normal wear and tear on materiel).

b. Required to elevate decisions to the next level in the chain of command after it is determined that controls available to him/her will not reduce residual risk to an acceptable level.

3. Accept Risk When Benefits Outweigh the Costs

All identified benefits should be compared to all identified costs. The process of weighing risks against opportunities and benefits helps to maximize organizational capability. Even high-risk endeavors may be undertaken when there is clear knowledge that the sum of the benefits exceeds the sum of the costs. Balancing costs and benefits may be a subjective process and open to interpretation. Ultimately, the balance may have to be determined by the appropriate decision maker.

4. Anticipate and Manage Risk by Planning

Risks are more easily assessed and managed in the planning stages of an operation/task. Integrating risk management into planning as early as possible provides the decision maker the greatest opportunity to apply ORM principles. Additionally, feedback must be provided to benefit future missions/activities.

G. ORM VS. TRADITIONAL APPROACH

Although the five steps of ORM are a lot like the decision-making process that good leaders have always used, applying a standard process is different in some important ways.

- ORM is more systematic. Frequently, hazard identification and assessment is random, and highly dependent upon an individual's past experience and organizational skills. ORM provides organized common sense and requires the operator(s) to focus on one piece of the puzzle at a time, completing each step before moving on to the next.

- ORM is more proactive. It requires an attempt to identify ALL hazards, not just the things that have happened in the past.

- ORM addresses all types of risk that could threaten our ability to accomplish the mission/task during the planning process (security, readiness, communications, enemy threats, fiscal limitations, credibility, health, personal safety, equipment failures, etc.) This allows effective prioritization of risks, which helps focus limited time/assets on the most important issues, rather than addressing safety threats as an after-thought, once the plan has been formulated.

- ORM enhances communication about risk by providing a common process and set of terms. It provides a means to articulate concerns and justify decisions.

Figure 2-5 summarizes the differences in the two approaches.

ORM	**vs.**	**Traditional Approach**
Systematic/Organized Common Sense		**Random, Individual-Dependent**
Proactive		**Reactive**
Integrates All Types of Risk Into Plan		**Safety as After-thought Once Plan is Done**
Common Process/Terms		**Non-standard**
Conscious Decision Based on Risk vs. Benefit		**"Can Do" Regardless of Risk**

Figure 2-5. ORM vs. Traditional Approach (From U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)

H. THE BENEFITS OF ORM

The U.S. Military has already garnered significant gains in terms of conserving assets and preventing injury to personnel. The following are some examples as cited by the U. S. Navy and Marine Corps School of Aviation Safety.

-Aviation Army's class A aircraft mishap rate was 0.64 in FY96, down 83% from their FY91 rates, and lower than any other service. The Army also demonstrated a 64% reduction in casualties during battalion training cycles, using risk management.

-In June 96, Navy Reserve Airwing CVWR-20 completed a highly successful embarkation on board the USS JOHN C. STENNIS (first time the entire wing embarked together in 6 years), including 3 days of cyclic night and day flight ops, with only two minor injuries (no lost work days).

- Marine Air Group MAG-13 has pioneered the use of a MacDonnell Douglas computer program which calculates risk of flights based on many factors, to include flight time, time of day, currency and proficiency in particular flight tasks, human factors, mission difficulty, etc.

- The USS GEORGE WASHINGTON Battle group also used ORM extensively during their very successful 1996 deployment. In addition to using a planning cell to look ahead 5 days and begin assessing the risks for upcoming operations, they encouraged identification of hazards by sister ships whenever they were along side. (Similar to the safety survey concept, hazards are sometimes more visible to an outsider than to those inside the organization.)

- Commander, Second Fleet began using ORM to evaluate and prioritize contingency-operation actions (COAs) based on operational mission hazards during their planning/execution for JTFX 97-2. Threats to the campaign exercise such as things that could cause combat casualties, loss of time, position or will of the forces to fight, etc. are evaluated using ORM, helping the staff to focus on the most important threats. They also are using a "benefit analysis" matrix like the risk assessment matrix to help them assess the benefits of particular COAs and weigh risk versus benefit.

- The leadership to Training Wings TRW-1 and TRW-6 met at Meridian with members of the NAVAIR and Test Pilot School teams to evaluate recent T-2 aircraft performance. During the course of the meetings they conducted a thorough risk assessment of returning the T-2 to flight status. The risk assessment included a complete review of past flight control anomalies, results of engineering investigations and a description of proposed aircraft modifications. The end result of the meeting was a measured three-phase approach to the resumption of T-2 flight operations.

- The USS NIMITZ Battle Group received ORM training approximately four months before conducting a 72-hour continuous flight operations exercise. They utilized the ORM process heavily in their planning for the July 1997 exercise. The exercise was completed with no material losses and two minor injuries.

I. ORM LEVELS OF APPLICATION

The amount of time and level of detail involved in the five steps of ORM varies, depending upon the circumstances.

1. Time-Critical

ORM entails a quick, mental review or discussion using five steps during the execution phase of operations/training and for crisis response planning.

2. Deliberate

ORM is a slightly expanded, more detailed application of the five steps in planning for an operation or reviewing procedures. This process level is used when there is a good understanding of the issues based on experience. The following list of ORM steps apply:

(1) Identify Hazards
  (a) Operation Analysis – a list or chart of the operation's major steps.
  (b) Preliminary Hazard Analysis (PHA) – a list of hazards and associated causes for each step of the operation analysis.
    (i) List negative consequences
    (ii) List vulnerabilities
    (iii) List possible causes
(2) Assess Hazards – prioritize identified hazards by severity and probability. Figure 2-3, Risk Assessment Code Chart, can be used to facilitate this.
(3) Make Risk Decisions
  (a) Consider Risk Control Options
    (i) Most Serious Risks First
    (ii) Refer to PHA Causes
  (b) Conduct a Risk vs. Benefit Analysis
  (c) Communicate as Required - If risks still out weigh benefits or additional resources are needed to implement selected controls, communicate this up the chain of command.
(4) Implement Controls
(5) Supervise

3. In-Depth

The five-step process for in-depth ORM is basically the same as that or the deliberate process, except that a more thorough risk assessment (first two of the five steps) is conducted, and a training realism assessment can be added if applicable. Some of the details of this level follow.

a. Risk Assessment

This risk assessment could involve research of available data, use of diagram and analysis tools, formal testing or long term tracking of the hazards associated with the operations. Examples of in-depth ORM applications include long-term planning of complex operations, introduction of new equipment, materials and missions, development of tactics and training curricula and major system overhaul or repair.

There are also a variety of in-depth hazard analysis tools that can be used. While a detailed discussion of each of these techniques is outside the scope of this thesis, they are listed to demonstrate the flexibility of the ORM process. They include:

- Analysis of Data

-Cause and Effect Diagram

-Tree Diagrams

-Surveys

-Simultaneously Timed Event Plotting (STEP)

-Failure Mode and Effects Analysis

-Interface Analysis

-Mapping

-Energy Trace and Barrier Analysis

b. Training Realism Assessment

The idea behind the Training Realism Assessment is to minimize the differences between training and actual combat procedures. It is based on the fact that a risk control that reduces training realism may increase risk to personnel and the mission in an actual combat situation.

The method:

1. Identify each control/procedure that is different from actual combat procedures.

2. Challenge each one to determine why it is different.

3. If the difference is valid (because of safety, resources, time, etc.), determine whether or not it has an undesired impact on training realism. Make adjustments to reduce undesired impact and identify any non-combat risk controls as "training only".

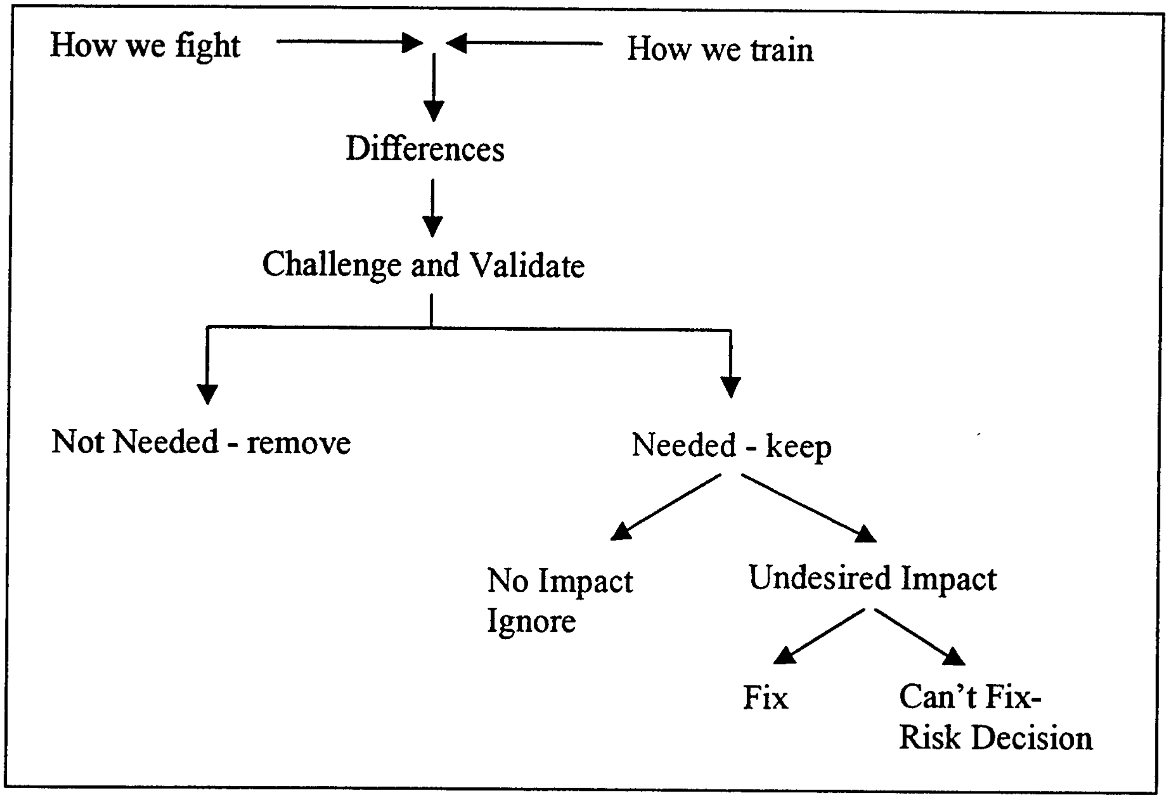


Figure 2-6. Training Realism Assessment (From U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)

Figure 2-6 depicts the Training Realism Assessment process, and can be used as a job aid to conduct the assessment.

If a risk control is needed, but it is not consistent with combat procedures, we must determine if there is a way to modify the control so that it can be used effectively in combat. A good example is the requirement for a safety observer. A separate safety observer often used in training will not be available in combat. However, we might be able to transfer the risk control functions of the safety observer to personnel in the chain of command to achieve an acceptable level of risk while eliminating the unrealistic aspect of the training. These risk control functions would then be in effect during both combat and training.

If the separate safety observer is necessary due to the level of risk and experience of the personnel involved, the unrealistic effects of having an observer might be reduced by placing the observer in a less visible position from which he could check and control, but not interfere with the operation.

Finally, if the control is required for training, and its adverse impact cannot be reduced, we must at least ensure the trainees recognize that it is for "training only."

J. ORM IMPLEMENTATION IN THE U.S. NAVY

The Chief of Naval Operations Instruction (OPNAVINST) 3500.39 is the guiding policy for implementation of ORM throughout the fleet. It has directed the following:

- All unit Commanding Officers should ensure that ORM is implemented into all levels of their commands.

- Train all personnel in the ORM process

- Incorporate identified hazards, assessments and controls into briefs, notices, and written plans.

-Conduct thorough risk assessments for all new or complex evolutions, defining acceptable risk and possible contingencies for the evolution.

The original concept of adapting ORM for use by the Navy was motivated by the need to improve safety in the high-risk environment of Naval Aviation. Therefore, that community has taken the lead in the practical implementation of ORM throughout the fleet through a three-phased approach. To Summarize:

-Phase I is the “Jump Start for Operational Units” that introduces ORM training into the fleet by getting senior naval aviation leadership knowledgeable about ORM, educating squadron leadership and assist squadrons in implementing it as quickly as possible. To facilitate this the Naval Safety Center has initiated Advanced ORM/Train-the-Trainer courses.

-Phase II starts the cradle to grave training philosophy by implementing it in the training command and undergraduate pilot training. The goal will be perpetual training required to keep ORM skills current in the fleet. It implements the cradle to grave philosophy by expanding fleet training to include participation by the Naval Aviation Training Command (NATRACOM). It starts with first educating Aviation Preflight Indoctrination (API) and training squadron instructors, followed by implementing ORM in the training squadrons themselves thus educating API and flight training students.

-Phase III expands ORM training into the all-persuasive Leadership continuum as well as enlisted maintenance training. ORM is an essential leadership tool for the entire Naval service; therefore, the proper place for the training to reside is in the Leadership Continuum where it will be taught at every level from E-5 to Prospective Commanding Officer (PCO).

III. INFORMATION ASSURANCE RISK MANAGEMENT (IARM)

A. THE NEED FOR IARM

There is opportunity to apply ORM principles to computer network security. The environment our computer networks operate in is full of hazards. Moonlight Maze, Operation "Eligible Receiver," the Melissa and "I Love You" viruses, and the distributed denial of service (DDOS) attacks performed on major web sites such as Yahoo and E-bay are ready examples. The DON has many computer networks, both ashore and at sea. While there is an accreditation process mandated by the Defense Information Technology Security Certification and Accreditation Program (DITSCAP), there are no standardized methods for senior decision makers, network administrators and users of these systems to make informed decisions concerning the risks these hazards pose up to or between accreditations. John Gilligan, chief information officer (CIO) at the Energy Department and co-chair of the CIO Council's committee on security, privacy and critical infrastructure has characterized the distributed client-server environment as more difficult to manage effectively, saying, "This is not a technical issue. It is a cultural issue at root." (Jackson)

ORM has demonstrated itself as a systematic way to proactively attempt to identify all hazards present in a given environment, not just those identified in the past. It addresses all types of risk that can have an adverse impact to the task at hand in the planning process. ORM enhances communications about risk, provides a common set of terms, and facilitates a means to articulate concerns and justify decisions made. The final result is a conscious decision to accept or reject the assessed risk based on the potential cost and benefit to the overall task. ORM can be applied anywhere. As the former Chief of Naval Operations (CNO) Admiral Jay Johnson put it: “ORM applies across the entire spectrum of naval activities, from joint operations and fleet exercises to daily routine. We must encourage top down interest in the ORM process, from the flag level all the way to the deckplates.”

B. THE IARM PROCESS - INTRODUCTION

IARM does not aim to eliminate the security risk inherent in information systems, nor computer networks in particular, but to facilitate a process by which those risk can be managed to minimize their adverse affects on the confidentiality, integrity and availability of information on computer network systems. As in ORM, it is presented as a standardized tool to aid users, IT support personnel and senior decision makers to *pro-actively* prevent security lapses. IARM adapts the five-step process of ORM in order to change people’s perception of security risk in their information systems’ environment by providing the best baseline of knowledge and experience available in which to make informed decisions. IARM minimizes security risks to acceptable levels by systematically applying controls to each risk that is not acceptable. It seeks to change cultural attitudes toward managing risk in a computer network environment by making information assurance the primary consideration when making decisions.

A useful illustration of how IARM approaches security differently is made by examining the approach the Navy Marine Corps Intranet (NMCI) is taking. The NMCI is a large contract entailing the massive outsourcing of the DON’s end-to-end information services requirements. The Program Executive Office Information Technology (PEO-IT) who is managing the NMCI contract acknowledges that along with increasing network connectivity, the potential for information warfare (IW) attacks also increases. The NMCI information fact file at http://peo-it.navy.mil/documents/nmci_security.pdf states:

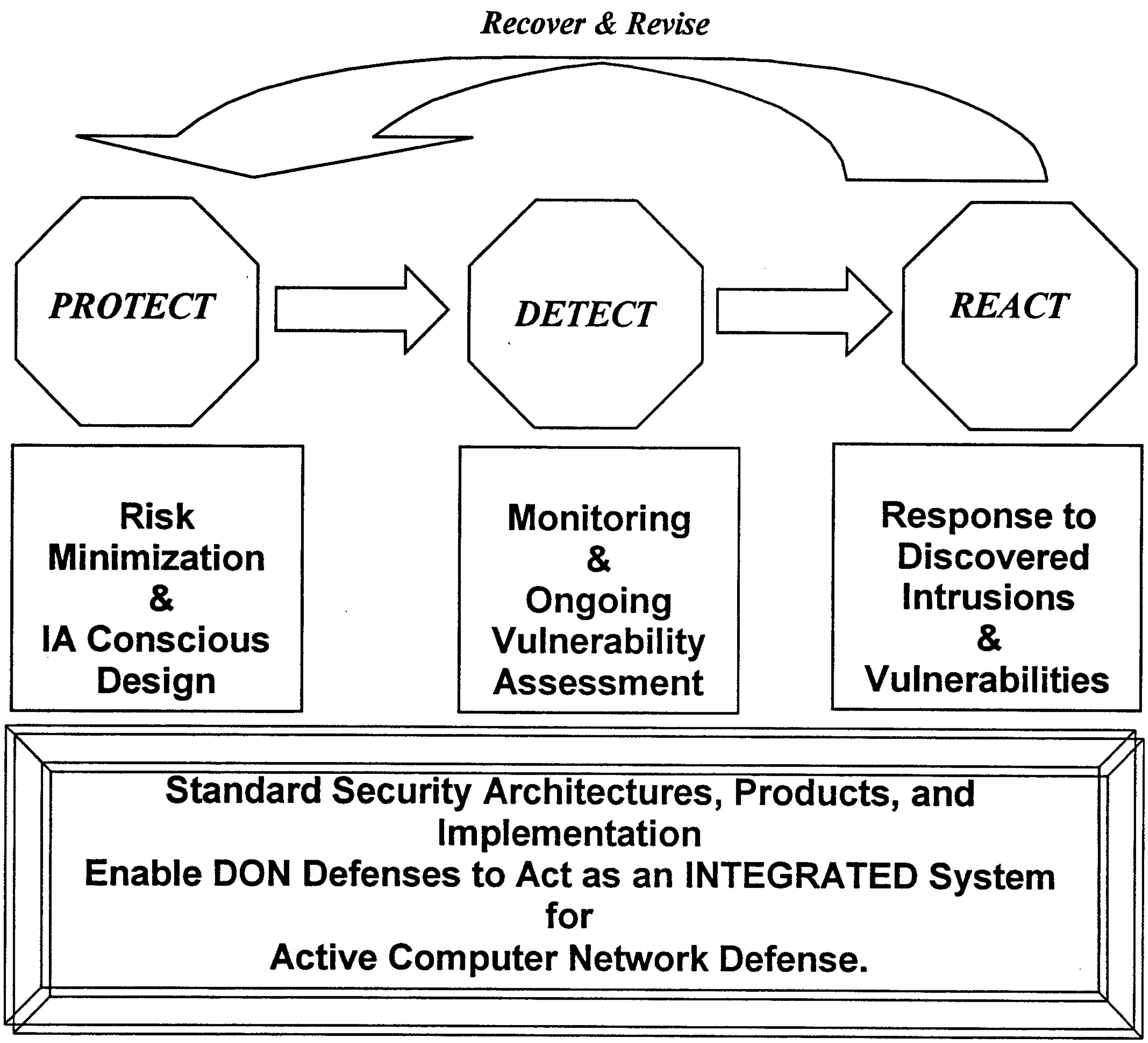
> To counter these threats, the DON will deploy an effective strategy (security architectures, policies, procedures and tactics) of aggressive *active* computer network defense within the NMCI structure.
>
> While perfect security in an information-sharing environment is nearly impossible, the NMCI will do much to minimize system vulnerabilities and counter potential threats. To this end, the DON has defined a Defense in Depth strategy that uses currently available protection *technology*, installed in a layered system of defenses... (emphasis by author)

The active computer network defense concept is illustrated in figure 3-1 below and is somewhat similar to IARM concepts.

While it is comforting to read that an "aggressive active computer network defense" will be pursued, the author's healthy skepticism leads him to believe that the vast majority of that defense will be technology based, possibly at the expense of user and decision maker training. An examination of the NMCI Service Level Agreements (SLA) concerning information assurance services makes no mention of security training. There is a separate SLA that addresses user training and indicates that 8 hours per year per user of information security training will be provided. The details of this training are unknown to the author. It is the author's opinion that if this training is offered in a "general-military training" (GMT) fashion, it will be difficult to tailor it to the three specific groups that are the major stake holders in the NMCI, users, DON IT support personnel, and DON decision makers.

The information security fact file cited above states "that only authorized Department of Defense (DoD) personnel will perform critical security roles." The author contends that user, IT support personnel, and decision maker *security* awareness, both military and contractor, is one of those critical roles. Implementing the IARM process and the recommendations above could be used to facilitate strengthening the human factors aspect of an active Computer Network Defense (CND).

Active Computer Network Defense: Both Developers and Operators are Critical Players



Recover & Revise

PROTECT

DETECT

REACT

Risk Minimization & IA Conscious Design

Monitoring & Ongoing Vulnerability Assessment

Response to Discovered Intrusions & Vulnerabilities

Standard Security Architectures, Products, and Implementation
Enable DON Defenses to Act as an INTEGRATED System
for
Active Computer Network Defense.

Figure 3-1. NMCI Active Computer Network Defense Concept (From SPAWAR Naval Intranet Concept Brief, Version 2, 30 May 1999)

C. IARM TERMS

The following are terms used in IARM in a computer network environment. They are presented to facilitate a more in-depth discussion on the five-step IARM process later in the terms of information assurance (IA).

1. Confidentiality

A security service used to provide assurance that information is not disclosed to unauthorized persons, processes, or devices. (CIAO, p.53)

2. Integrity

A security service that ensures an information system (IS) operates without unauthorized modification, alteration, impairment, or destruction of any of its components. (CIAO, p.55)

3. Authentication

A security service or measure designed to establish the validity of a transmission, message, or originator; or as a means of verifying a user's authorization to access specific types of information. (CIAO, p.51)

4. Non-repudiation

A security service that prevents either a sender or receiver of transmitted data from legally denying its transmission or reception. (Stallings, p.10)

5. Availability

A security service that ensures timely and reliable access to data and information services for authorized users. (CIAO, p.51)

6. Access Control

A security service that limits and controls the access to information system (IS) resources to authorized users, programs, processes, or other systems. (CIAO, p.51)

7. Exposure

A form of possible loss or harm in a computing system (e.g., loss of one of the services defined above). (Pfleeger, p.3)

8. Vulnerability

A flaw in security procedures, software, internal systems controls, or implementation of an IS that may cause any of the security services (i.e., those services defined above) to be degraded or defeated. Vulnerabilities include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters. (CIAO, p.59)

9. Threat

Any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service or physical destruction or impairment. (CIAO, p.58) Any attack that takes advantage of a vulnerability (buffer overflow, social engineering, spoofing, eavesdropping, etc.).

10. Risk

An expression of possible data or information loss or compromise in terms of severity and probability.

11. Severity

The worst, credible consequence that can occur as a result of a vulnerability. It is the potential degree of data or information loss or compromise.

12. Probability

The likelihood that a vulnerability will result in data loss or compromise based on factors such as physical location, network services provided, network protocols, operating systems, personnel, and historical information. An expression of the possibility of a successful exploitation.

13. Risk Assessment

The process of detecting vulnerabilities and assessing associated risk. It is the first two steps of the IARM process. The result can be a risk assessment code (RAC) derived from the chart in figure 3-2.

14. Control

A method for reducing risk for an identified vulnerability by lowering the probability of occurrence, decreasing potential severity, or both.

15. Information Systems

All the electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information. An IS may be automated (e.g., a computerized information system) or manual (e.g., a library's card catalog). (CIAO, p.55)

16. Information Operations

Actions taken to affect an adversary's information and information systems while defending one's own information and information systems. (CIAO, p.54)

17. Information Assurance

Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

18. Information Assurance Risk Management

The process of dealing with risk to information and data that is inherently associated with information operations and information systems, which includes risk assessment, risk decision-making, and implementation of effective risk controls.

D. CAUSES OF RISK IN INFORMATION SYSTEMS SECURITY

A discussion of some of the threats and vulnerabilities that make using information systems a risky endeavor is useful. It facilitates a more thorough understanding of how threats are ever present in computer network and other environments, and how users and IT support personnel using IARM to control risks associated with those threats can be more effective in identifying them.

1. Threats

Threats can be categorized by associating them with the function that a computer network system provides, an uninterrupted flow of information. (Stallings, p.7) Figure 3-2 depicts the threats discussed below.

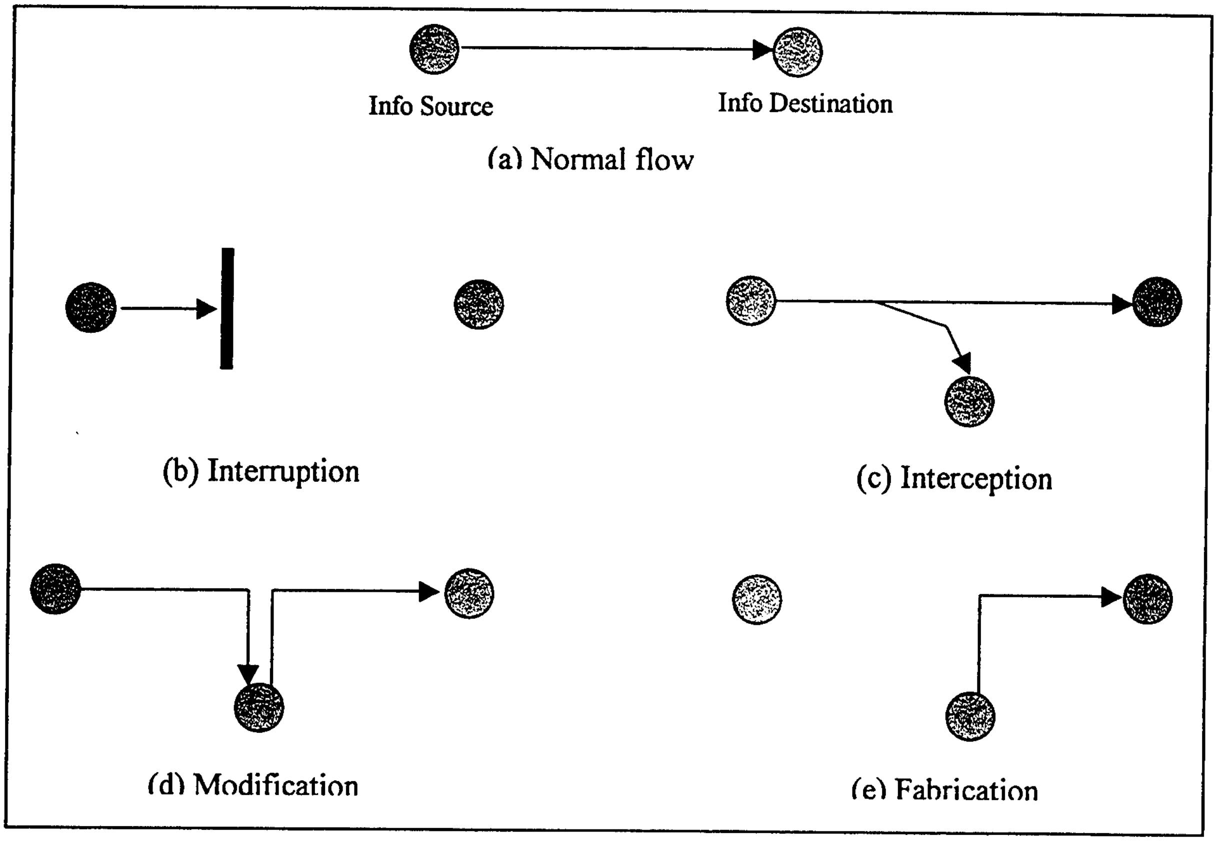


Figure 3-2. Security Threats (From Stallings, p. 7)

a. Interruption - Commonly known as a denial of service (DOS), this threat is an attack on availability. Examples include cutting a communication line, destruction of hardware, "smurf" and "syn flood" attacks, distributed denial of service attacks (DDOS), jamming and viruses that destroy data on hard drives.

b. Interception - Commonly known as sniffing, this threat is an attack on confidentiality. Examples include keyboard loggers, network sniffers, traffic analysis (TF), traffic flow analysis (TFA), and the unauthorized copying of data.

c. Modification - Commonly known as the "man-in-the-middle," this threat is an attack on integrity. Examples include altering data files through the use of

Trojan horse programs, replay attacks and altering contents of messages being transmitted.

d. Fabrication - Commonly known as "masquerading," this threat is an attack on authenticity. Examples include impersonating legitimate users through the use of "back door" programs to gain access to host computers, the installation of "root" kits, adding spurious messages to a network, or records to a file.

e. Social Engineering – A threat not directly depicted in the figure above, but is worthy of discussion. This threat does not attempt to exploit the technology of a network, but the people who interact with it. Social Engineering is the term used to describe an attempt to manipulate or trick a person into providing valuable information or access to that information. It attempts to take advantage of people's desire to be helpful. A possible example could be someone identifying themselves as a senior officer over the phone to their command and asking the password to their account be changed because they are on travel. A very junior person might be duped into performing the requested action. Social engineering can be computer based as well. Consider a user on a computer who suddenly sees a message that their connection to the network has timed out and they need to log back in. This method has been used in the past to collect passwords. (Cole, p.1-11)

Eric Cole, an instructor with the SANS institute, describes this to be one of the most difficult attacks to defend against. There is no technology available today that can keep a person from unwittingly divulging information. The best defense is clearly written security policies and educating users about this and different threats.

2. Vulnerabilities

Scrambay, McClure, and Kurtz list the "Top 14 Security Vulnerabilities" in their very popular book, *Hacking Exposed: Second Edition.* (p. 662) They are listed below:

a. Inadequate router access control: Misconfigured router access control lists (ACLs) can allow information leakage through ICMP, IP, NetBIOS, and lead to unauthorized access on your DMZ servers.

b. Unsecured and unmonitored remote access points provide one of the easiest means of access to your corporate network. Telecommuters often connect to the Internet with little protection, exposing sensitive files to attack.

c. Excessive trust relationships such as NT Domain Trusts and Unix .rhost and hosts.equiv files can provide attackers with unauthorized access to sensitive systems.

d. User or test accounts with excessive privileges.

e. Software that is unpatched, outdated, vulnerable, or left in default configurations.

f. Hosts running unnecessary services (such as RPC, FTP, DNS, SMTP) are easily compromised.

g. Excessive file and directory access controls (NT shares, UNIX NFS exports).

h. Unauthorized services like X Windows allow users to capture remote keystrokes.

i. Weak, easily guessed, and reused passwords at the workstation level can doom your servers to compromise.

j. Misconfigured Internet servers, especially CGI scripts on web servers and anonymous FTP.

k. Misconfigured firewall or router ACL can allow access to internal systems directly or once a DMZ server is compromised.

l. Lack of accepted and well-promulgated security policies, procedures and guidelines.

m. Information leakage can provide the attacker with operating system and application versions, users, groups, shares, DNS information via zone transfers, and running services like SNMP, telnet, rusers, rpcinfo, NetBIOS.

n. Inadequate logging, monitoring, and detection capabilities at the network and hosts level.

The SANS Institute maintains a continually updated list on what industry, government and academia consider to be the top-ten, current vulnerabilities at http://www.sans.org/topten.html. Worth noting is that this web site refers to each vulnerability by its CVE or CAN number as assigned by http://cve.mitre.org. This facilitates a common terminology in discussing the details of a new exploit. Finally, and most importantly, the SANS site also contains links to vendors that offer software patches to combat these exploits.

It is interesting to note that the above includes non-technical issues that can apply to all types of information systems. The above lists are also an insight to the impressive number of vulnerabilities and exploits that network IT support personnel, security personnel, and decision makers must be able to recognize, understand, protect against, and recover from if need be.

E. IARM PROCESS

The IARM process is a simple five-step process. It is a continuous process designed to detect, assess, and control risk to information while qualitatively enhancing computer network defense (CND) performance and maximizing network capabilities. It is adapted from the concept of applying a standard, systematic approach to minimizing risk that was originally developed to improve safety in the development of weapons, aircraft, space vehicles, and nuclear power and is used throughout the Navy in Operational Risk Management (ORM). The five steps are:

1. Identify Vulnerabilities

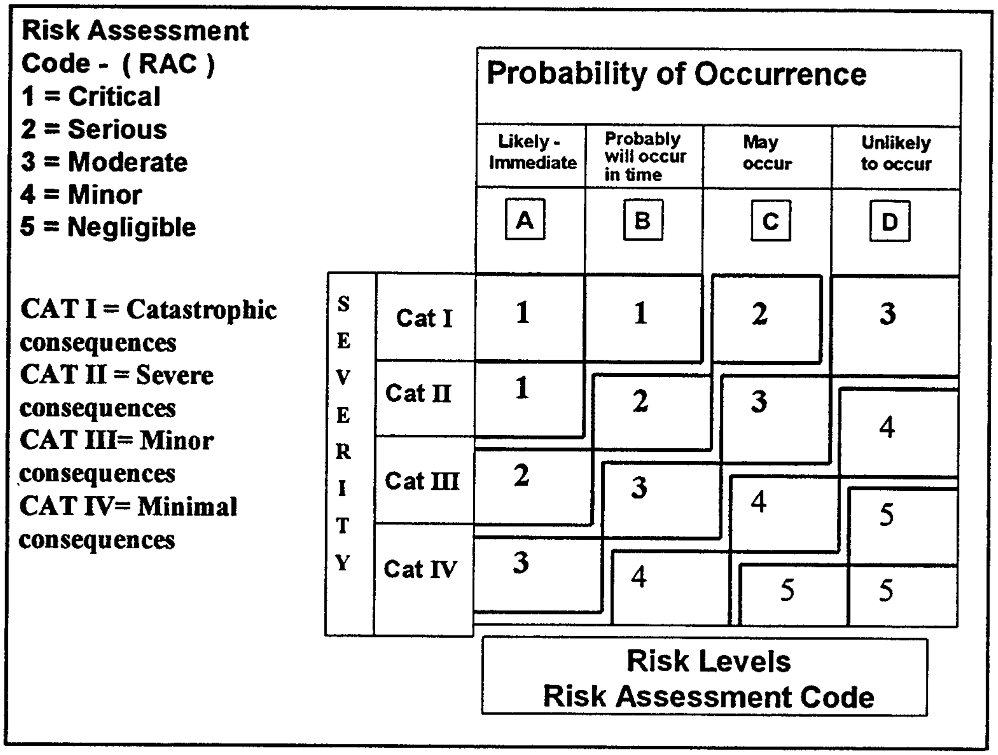
Identify potential causes of compromise to information in terms of confidentiality, integrity and availability. Specific actions include identifying computer network assets and listing vulnerabilities in terms of its effects on security services. Assets can include hardware, software, data, services, people, documentation, policies and supplies. (Pfleeger, p.464) A table, as shown in Table 3-1, can be used to organize the association of vulnerabilities and assets.

ASSET	CONFIDENTIALITY	INTEGRITY	AVAILABLITY
Hardware			
Software			
Data			
Services			
People			
Policies			
Documentation			

Table 3-1. Assets and Security Services (After Pfleeger)

2. Assess Vulnerabilities

For each vulnerability identified, determine the associated risk in terms of severity and probability. Specific actions include assessing the exposure, severity and probability to the vulnerabilities listed in step 1. The Risk Assessment Code (RAC) chart in figure 3-3 can be used to accomplish this step.



Risk Assessment Code - (RAC)
1 = Critical
2 = Serious
3 = Moderate
4 = Minor
5 = Negligible

CAT I = Catastrophic consequences
CAT II = Severe consequences
CAT III= Minor consequences
CAT IV= Minimal consequences

SEVERITY	Probability of Occurrence			
	Likely - Immediate	Probably will occur in time	May occur	Unlikely to occur
	A	B	C	D
Cat I	1	1	2	3
Cat II	1	2	3	4
Cat III	2	3	4	5
Cat IV	3	4	5	5

Risk Levels
Risk Assessment Code

Figure 3-3. IARM Risk Assessment Code Chart (After U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)

Using this matrix does not lessen the inherently subjective nature of risk assessment, however a matrix does afford a consistent framework for evaluating risk. Although different matrices may be used for various applications, any risk assessment tool should include the elements of vulnerability severity and threat probability. The RAC defined by a matrix represents the degree of risk associated with a vulnerability considering severity and probability. While the degree of risk is subjective in nature, the RAC does accurately reflect the relative amount of risk perceived between various vulnerabilities. Using the matrix, the RAC is derived as follows:

a. Vulnerability Severity – An assessment of the worst credible consequence that can occur as a result of a vulnerability. Severity is defined by potential degree of information compromise, or loss of information all together (e.g., denial of service). The combination of two or more vulnerabilities may increase the overall risk. Vulnerability categories are assigned as Roman numerals according to the following criteria:

(1) Category I – The vulnerability may cause catastrophic loss of information or grave damage to national interest.

(2) Category II – The vulnerability may cause severe loss of information, severe damage to national or service interests, or severe degradation to efficient use of information.

(3) Category III – The vulnerability may cause minor loss of information, minor damage to national, service, or command interests, or minor degradation to efficient use of information.

(4) Category IV - The vulnerability may cause a minimal loss of information, minimal damage to national or service interests, or minimal degradation to efficient use of information.

b. Exploitation Probability – the probability that a vulnerability will result in an actual exploitation (some degree of compromise of data or denial of service), based on an assessment of such factors as location, exposure, affected population, experience, or previously established statistical information. Exploitation probability will be assigned will be assigned an English letter according to the following criteria:

(1) Sub-category A – Likely to occur immediately or within a short period of time. Expected to occur frequently to a computer network, servers, host or client.

(2) Sub-category B – Probably will occur in time. Expected to occur several times to a computer network, server, host or client.

(3) Sub-category C – May occur in time. Can reasonably be expected to occur sometime to a computer network, server, host or client.

(4) Sub-category D – Unlikely to occur.

c. Risk Assessment Code – The RAC is an expression of risk that combines the elements of vulnerability severity and exploitation probability. The RAC is expressed as a single Arabic numeral that can be used to help determine vulnerability control priorities. Note that in some cases, the worst credible consequence of a vulnerability may not correspond to the highest RAC for that vulnerability. For example, one vulnerability may have two potential consequences (loss of confidentiality - I and non-repudiation - III). The severity of the worst consequence (loss of confidentiality) may be unlikely (D), resulting in RAC 3. The severity of the lesser consequence (III) may be likely (A), resulting in a RAC of 2. Therefore, it is also important to consider less severe consequences of a vulnerability if it is more likely than the worst credible consequence, since the combination may present greater overall risk. (OPNAVINST 3500.39, p. 7)

3. Make Risk Decisions

Develop risk control options, and then decide if benefits outweigh risks. Start with the most serious risk first. Specific actions include identifying control options, determining the effects of those controls, prioritizing risk control measures, selecting risk controls and making risk decisions. If risk outweighs benefit, or if assistance is required to implement controls, seek further controls or guidance from superiors.

4. Implement Controls

Once the risk decisions are made, implement selected controls. Specific actions include making implementation of the above controls clear, establishing accountability, and providing support. If the control entails a new IT technology like implementing a

Virtual Private Network (VPN) for network traffic confidentiality, then it is vital that an investment be made into the people who will maintain and use it as well. A grouping of controls can be as follows:

a. Controls that implement confidentiality, integrity, authentication and non-repudiation: Public Key Infrastructure (PKI), secure protocols (IPSec), secure e-mail (PGP), network integrity controls (intrusion detection systems), operating system protection features (anti-virus software), Secure Shell (SSH), etc. These controls are most applicable to implementations at the application level.

b. Controls that implement availability and access controls: network access controls (firewalls), secure-socket layer (SSL), identification, database and operating system access controls, etc. These controls are most applicable to implementations at the transport and network levels.

c. Controls that protect the physical medium of transmission: link cryptography, spread-spectrum (low probability of detection and interception techniques (LPD and LPI)), etc. These controls are most applicable to the physical and data link levels.

5. Supervise

Some method of testing must be devised to ensure that the selected controls are performing as needed. A well-designed vulnerability assessment can satisfy this need. Care must be taken to watch for changes that could impact the original assumptions of the risk assessment. A change of this nature usually warrants initiating the IARM process again. Other specific actions include supervising the control implementation, continuously monitoring for effectiveness, and collecting feedback from non-involved IT support personnel and users. A summary of specific actions associated with each step of the IARM process is given below in figure 3-4.

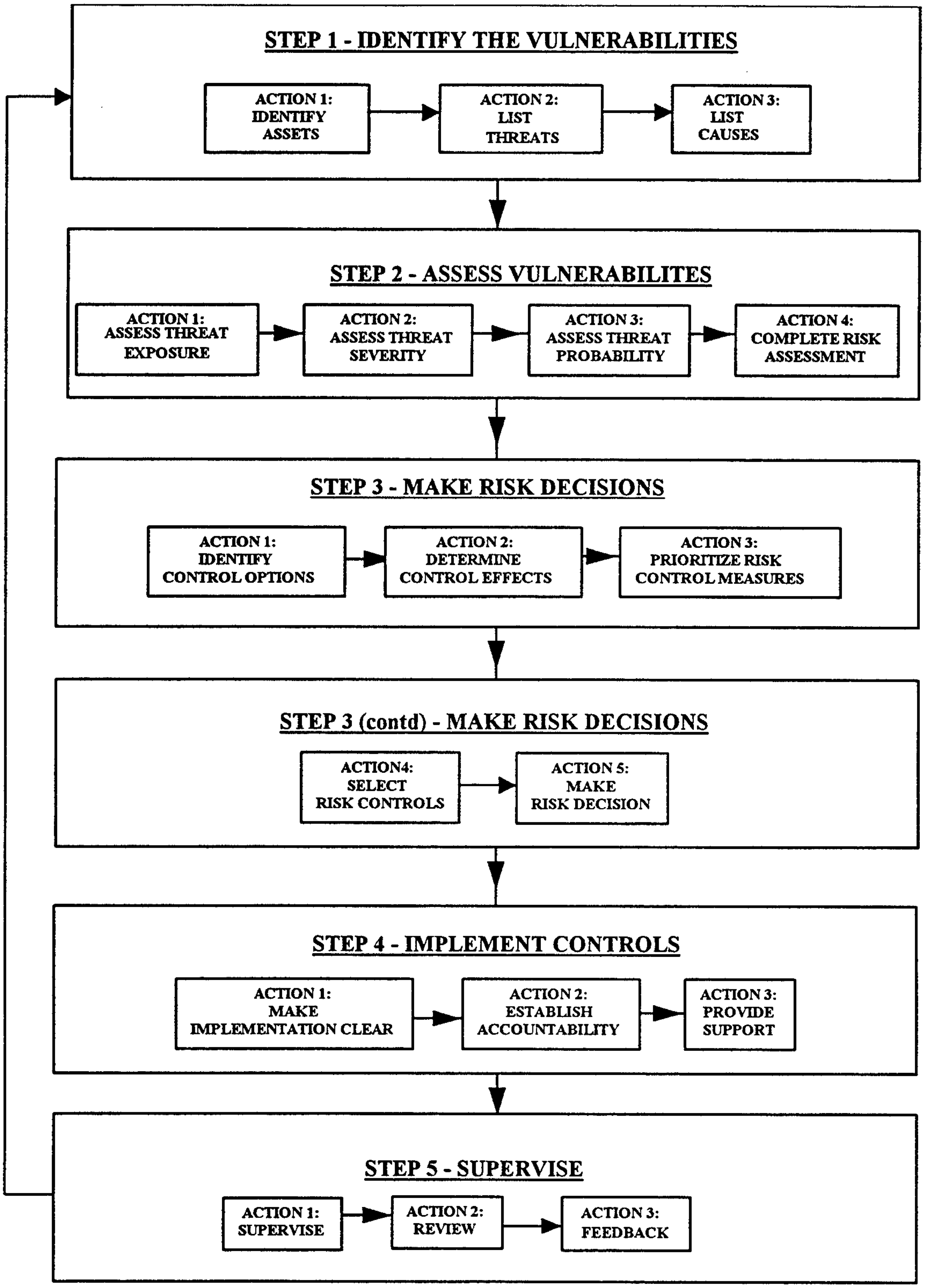

STEP 1 - IDENTIFY THE VULNERABILITIES
ACTION 1: IDENTIFY ASSETS
ACTION 2: LIST THREATS
ACTION 3: LIST CAUSES
STEP 2 - ASSESS VULNERABILITES
ACTION 1: ASSESS THREAT EXPOSURE
ACTION 2: ASSESS THREAT SEVERITY
ACTION 3: ASSESS THREAT PROBABILITY
ACTION 4: COMPLETE RISK ASSESSMENT
STEP 3 - MAKE RISK DECISIONS
ACTION 1: IDENTIFY CONTROL OPTIONS
ACTION 2: DETERMINE CONTROL EFFECTS
ACTION 3: PRIORITIZE RISK CONTROL MEASURES
STEP 3 (contd) - MAKE RISK DECISIONS
ACTION4: SELECT RISK CONTROLS
ACTION 5: MAKE RISK DECISION
STEP 4 - IMPLEMENT CONTROLS
ACTION 1: MAKE IMPLEMENTATION CLEAR
ACTION 2: ESTABLISH ACCOUNTABILITY
ACTION 3: PROVIDE SUPPORT
STEP 5 - SUPERVISE
ACTION 1: SUPERVISE
ACTION 2: REVIEW
ACTION 3: FEEDBACK

Figure 3-4. The Cyclic IARM Process (After U.S. Air Force ORM Process)

F. THE FOUR IARM PRINCIPLES

These principles, as with ORM, are indispensable to making effective decisions concerning risk. They govern all actions associated with risk management. These principles are applicable before, during, and after all aspects of managing, maintaining, and developing computer network systems. They are listed again here.

1. Accept No Unnecessary Risk

Unnecessary risk comes without a commensurate return in terms of real benefits or available opportunities. Using and maintaining computer network systems involve risk to information. The most logical choices for interacting with these systems are those that meet all mission/task requirements with the minimum acceptable risk. The corollary to this axiom is "accept necessary risk" required to successfully complete the mission or task.

2. Make Risk Decisions at the Appropriate Level

Making risk decisions at the appropriate level establishes clear accountability. Those accountable for the success or failure of the task must be included in the risk decision process. The appropriate level for risk decisions is the one that can allocate the resources to reduce the risk or eliminate the threat and implement controls. Typically, the commander, leader, or individual responsible for executing the mission or task is:

a. Authorized to accept levels of risk typical of the planned operation/task (i.e., possible loss or compromise of data and equipment, potential compromise of normal services offered).

b. Required to elevate decisions to the next level in the chain of command after it is determined that controls available to him/her will not reduce residual risk to an acceptable level.

3. Accept Risk When Benefits Outweigh the Costs

All identified benefits should be compared to all identified costs. The process of weighing threats against potential vulnerabilities helps to maximize computer network defense (CND) performance. Even high-risk endeavors may be undertaken when there is clear knowledge that the sum of the benefits exceeds the sum of the costs. Balancing costs and benefits may be a subjective process and open to interpretation. Ultimately, the balance may have to be determined by the appropriate decision maker.

4. Anticipate and Manage Risk by Planning

Vulnerabilities and threats are more easily assessed and managed in the planning stages of maintaining, updating, or developing computer networks. Integrating risk management into these activities as early as possible provides the decision maker the greatest opportunity to apply IARM principles. Additionally, feedback must be provided to benefit future computer network related activities.

G. IARM VS. TRADITIONAL APPROACH

Although the five steps of IARM are a lot like the decision-making process that good, security-knowledgeable IT support personnel would always use, applying a standard process is different in some important ways.

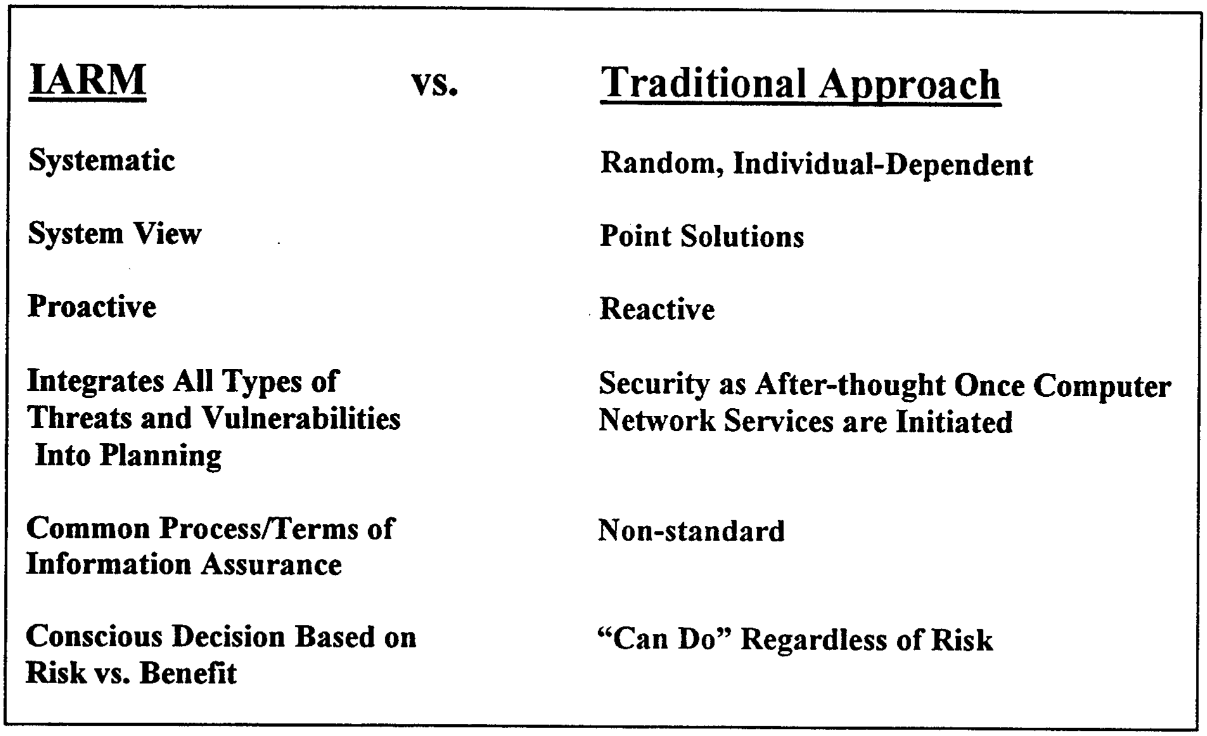
- IARM is more systematic. Frequently, threat identification and vulnerability assessment is random, and highly dependent upon an individual's past experience and computer network skills. IARM requires users, IT support personnel and decision makers to focus on threat at a time, shoring up that vulnerability before moving on to the next.

- IARM is more proactive. It requires an attempt to identify ALL threats and potential exploits, not just the ones that have occurred on that computer network in the past.

- IARM addresses all types of threats and vulnerabilities that could threaten our ability to keep network security services unimpaired (social engineering, virus detection, configuration management, user awareness, fiscal limitations, credibility, physical security, computer equipment failures, etc.) This allows effective prioritization of computer network related risks, which helps focus limited time/assets on the most important issues, rather than addressing security threats as an after-thought, once the policies have been formulated or computer network systems created.

- IARM enhances communication about threats and vulnerabilities by providing a common process and set of terms. It provides a means to articulate concerns and justify decisions to those who may not be completely aware or knowledgeable on the risks entailed in using computer networks.

Figure 3-5 below summarizes the differences in the two approaches.



IARM	vs.	Traditional Approach
Systematic		Random, Individual-Dependent
System View		Point Solutions
Proactive		Reactive
Integrates All Types of Threats and Vulnerabilities Into Planning		Security as After-thought Once Computer Network Services are Initiated
Common Process/Terms of Information Assurance		Non-standard
Conscious Decision Based on Risk vs. Benefit		"Can Do" Regardless of Risk

Figure 3-5. IARM vs. Traditional Approach (After U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)

H. IARM LEVELS OF APPLICATION

IARM is intended to be applied by all people who use, maintain, and manage information, as well as the computer network systems that may hold that information. Users, IT support personnel, and decision makers will thus devote different amounts of time and level of detail to the five steps of IARM, depending upon the circumstances.

1. Time-Critical

In this case IARM entails a quick, mental review or discussion using the five steps during the conduct of an activity, or for crisis response planning. As an example, a user may receive an e-mail with an attachment that looks suspicious because it contains more than two extensions (e.g., jpg.vbs). Should the user open the attachment? If it is not directly addressed in the unit's computer network use policies, the user may do a quick, mental run through of the five steps:

(1) Identify Vulnerabilities: The e-mail attachment may contain a malicious program that could spread, unauthorized to other machines within the organization (attack on integrity).

(2) Assess Vulnerabilities: What's the worst that could happen? The malicious program may be a Trojan for use by an intruder to gain access to other hosts, or a program to wipe out data on host computer within the organization (attack on availability). Since the user has had some information assurance awareness training, (i.e., IARM), they are aware that there is a likely occurrence, and thus a significant threat.

(3) Make Risk Decisions: Given the above quick analysis, the user now needs to determine if there is an operational need to open the attachment now. If the user has the authority to make that risk decision, one is made (i.e., open it now or not). In the absences of such authority, the user would go up his/her chain of command. In this case, the user does not have the authority to make the risk decision, he/she notifies technical support.

(4) Implement Controls: By not opening the attachment, or moving the attachment to an isolated system for investigation, the user is implementing the control (i.e., not opening suspicious attachments).

(5) Supervise: The user is exercising self-supervision by being vigilant for such situations in the future and sharing the experience with fellow personnel.

2. Deliberate

IARM is a slightly expanded, more detailed application of the five steps suited for planning for an operation or reviewing procedures. This process level is used when there is a good understanding of vulnerabilities based on experience and is summarized below.

(1) Identify Vulnerabilities
(a) Operation Analysis – an analysis of the specific computer network's services and protocols involved to accomplish them.
(b) Preliminary Hazard Analysis (PHA) – a list of vulnerabilities and associated causes for each step of the operation analysis.
(i) List negative consequences
(ii) List vulnerabilities
(iii) List possible causes
(2) Assess Vulnerabilities - using a matrix similar to the one in figure 3-1 can facilitate this.
(3) Make Risk Decisions
(a) Consider Risk Control Options
(i) Most Serious Risks First
(ii) Refer to PHA Causes
(b) Conduct a Risk vs. Benefit Analysis
(c) Communicate as Required - If risks still out weigh benefits or additional resources are needed to implement selected controls, communicate this up the chain of command.
(4) Implement Controls
(5) Supervise

3. In-Depth

The five-step process for in-depth IARM is basically the same as that or the deliberate process, except that a more thorough vulnerability assessment (first two of the five steps) is conducted, and a training realism assessment can be added if applicable. The following can be some of the details that apply.

a. Vulnerability Assessment

This vulnerability assessment could involve research of available data, use of diagram and analysis tools, formal testing or long term tracking of the vulnerabilities associated with the operations of the computer network system. Examples of in-depth

IARM applications include long-term planning of complex computer network operations, introduction of new computer equipment, materials and missions, protocols, training curricula, and major computer network system overhaul or repair.

While there are a variety of automated vulnerability assessment tools that can be used to test current systems, there are also a variety of in-depth vulnerability analysis tools that can be used in the risk management portion of the development phase of a computer network system. The following techniques can be applied to established systems. While a detailed discussion of each of these techniques is outside the scope of this thesis, they are listed to demonstrate the flexibility of the IARM process. They include:

- Analysis of Data
- Cause and Effect Diagram
- Tree Diagrams
- Surveys
- Simultaneously Timed Event Plotting (STEP)
- Failure Mode and Effects Analysis
- Interface Analysis
- Mapping
- Energy Trace and Barrier Analysis

b. Training Realism Assessment

The idea behind the Training Realism Assessment is to minimize the differences between training and actual combat procedures. We in the military must be able to deal with scenarios that may include other aggressive, overt actions in conjunction with a computer network attack (CNA). It is based on the fact that a risk control that reduces training realism may increase risk to personnel and the mission in an actual combat situation.

The method:

1. Identify each control/procedure that is different from actual combat procedures.

2. Challenge each one to determine why it is different.

3. If the difference is valid (because of safety, resources, time, etc.), determine whether or not it has an undesired impact on training realism. Make adjustments to reduce undesired impact and identify any non-combat risk controls as "training only".

Figure 3-6 depicts the Training Realism Assessment process, and can be used as a job aid to conduct a realistic, operational vulnerability assessment.

If a risk control is needed, but it is not consistent with combat procedures, we must determine if there is a way to modify the control so that it can be used effectively in combat. An example might be making certain critical network systems off-limits to red teams during actual joint-fleet exercises for fear of degrading the over-all exercise. Designating a network system, or a portion of it, off-limits will obviously not be an option available in combat. However, we might be able to transfer the risk control functions of the need for a critical portion of the network to other systems or platforms within the exercise to achieve an acceptable level of risk while eliminating the unrealistic aspect of the training. These risk control functions would then be in effect during both combat and training.

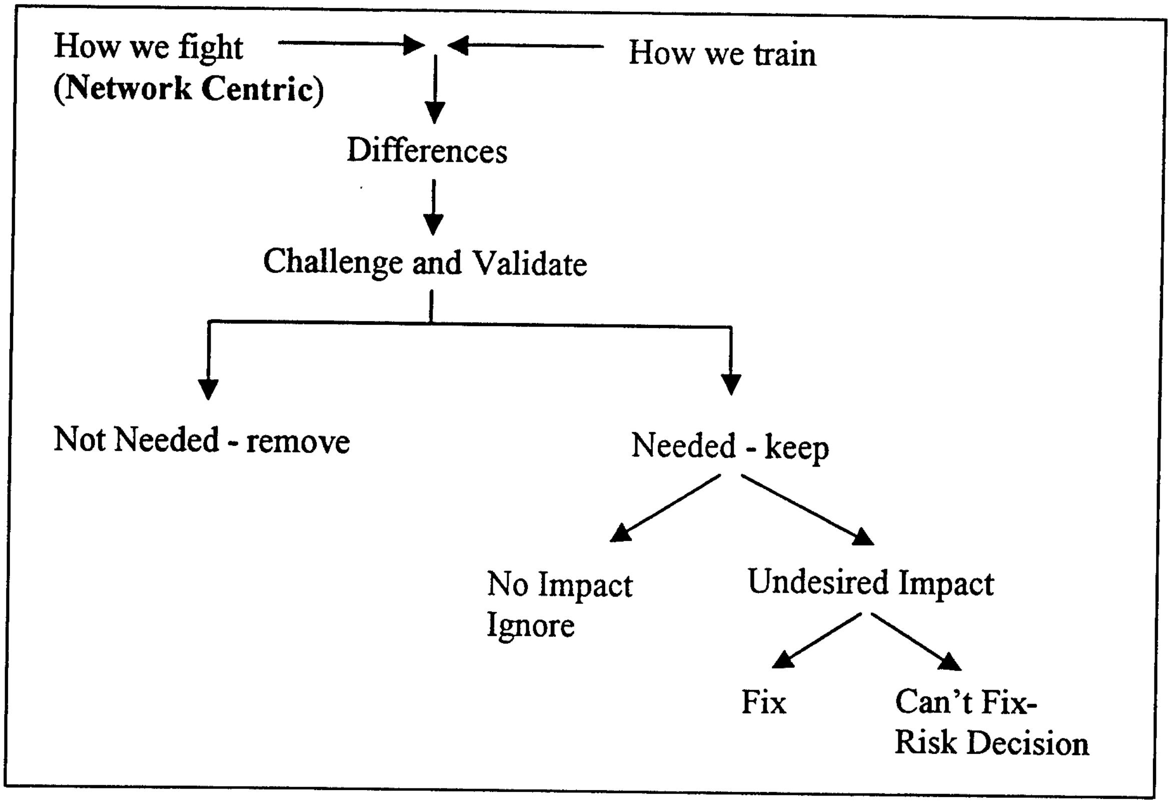


Figure 3-6. Training Realism Assessment (After U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)

If making a critical portion of the network off-limits to red teams is necessary due to the level of risk and experience of the personnel involved, the unrealistic effects of placing a critical network system off limits may be reduced by placing controls on the actual attacks a red team may simulate so as not to interfere with the overall operation.

Finally, if the control is required for training, and its adverse impact cannot be reduced, we must at least ensure the trainees recognize that it is for "training only."

c. IA Implementations for Systems

Defining requirements is a very difficult task when making procurement decisions for information systems (IS). An IS's performance, usability, and interoperability are often degraded by the requirement for the IA services described earlier. Likewise, trying to first determine what the IA requirements are, and then second, communicate those requirements to the system engineers and software developers who will actually design the implementations, can be as equally daunting. IARM's promotion of common IA terms can be used to establish IA criteria on which procurer and developer can agree upon before IA requirements are determined. Once requirements are determined, the in-depth IARM process can be used to analyze the effectiveness of the proposed solutions in each cycle of the procurement process.

A possible framework for presenting the IA requirements of some future IP-based information system implementation is illustrated below in figure 3-7.

ISO Layer	**Security Problem**	**Possible Solutions**
Application	Enforce: Application, Confidentiality, Authenticity, Integrity, Non-Repudiation of Data	SSH, PKI, S/MIME, PGP, Access Controls
Transport/ Network	Enforce Network-Based Confidentiality, Authenticity, Integrity, Perimeter Defense	Firewall, IDS, SSL, Access Controls, IPSec, VPN
Data Link/ Physical	Prevent Traffic Analysis (TA) and Traffic Flow Analysis (TFA), Iinterception, Jamming	Spread Spectrum, LPD/ LPI, Link Crypto

Figure 3-7. Framework for Determining IA Requirements and Implementations for a Future IP-Based Information System

The above model lends itself to a logical division of developmental expertise. The application level requirements would be under the purview of software developers while the remaining two levels would fall under network design engineers. The above model also illustrates the utility of pushing many of the IA services needed as far up the ISO model as possible to promote interoperability. Likewise, we can see the utility and value of securing the *data* instead of concentrating on securing the "plumbing."

After initial requirements and implementations are agreed upon, in-depth IARM can further be used by PMs (Program Manager) and IPTs (Integrated Procurement Teams) to justify the possible increase in cost or degradation in usability/interoperability those IA requirements can cause.

I. BENEFITS OF IARM

Though IARM, and risk management in general, is not very precise, it does offer benefits which can enhance a computer network system's defensive performance, in addition to those benefits listed above. It improves general network and information assurance awareness among users, IT support personnel and decision makers. Discussing issues of security can raise the general level of interest and concern. IT support personnel and decision makers may now have a comprehensive list of assets and vulnerabilities associated with those assets where none existed before. Decision makers now have an improved basis for implementing controls, justifying those controls which may prove inconvenient or expensive, and continuing the search for more effective controls should the need arise. Finally, IARM is a continuous, non-static process that can be applied by users, IT support personnel and decision makers alike, giving the whole chain of command the opportunity to personally make a positive contribution to the Department of the Navy's computer network defense performance. (Pfleeger, p.463)

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSIONS

A. VISION FOR IARM IMPACT ON OPERATIONS

As the U.S. Navy moves forward with initiatives like IT-21, NMCI, and Network Centric Warfare, every command should be preparing for the inevitable deployment of IP-based communication systems. These systems will be exposed to many of the same threats and vulnerabilities that occur in corporate America, and on the Internet at large, making Computer Network Defense (CND) an area of critical operational importance. While there will undoubtedly be very clever and creative ways to technically master the information assurance issues of tomorrow, one area that has remained resistant to technological remedies will always be present – the human factor. As we have seen in Naval Aviation, much ingenuity and resources have been poured into making our weapons platforms safe to operate, yet Naval Aviation continued to suffer significant mishaps. With the incorporation of ORM, Naval Aviation, and the Fleet at large, has been able to concentrate on the human factors side of mishaps and bring about the safest period in our Navy's history. Safety has become the premier concern in making decisions about risk, and the lessons that Naval Aviation learned can be applied in the area of information assurance as well. It is culture and attitudes that are most difficult to change. As a process focused on people, IARM can facilitate a paradigm shift in the way that the DON develops and uses computer network systems so that information assurance is quantifiably executable when interacting with computer network systems.

At the core of IARM, like ORM, is the goal of increasing the ability to make informed decisions by providing the best baseline of knowledge and experience available, through continuous and open communication.

B. ESTABLISHING A KNOWLEDGE BASE

One of the key elements that has made the Naval Aviation Safety Program effective is the establishment of a detailed mishap and hazard reporting system. This system facilitates the establishment of a knowledge base of mishap and hazard causes, recommendations for correcting the determined causes, and a mechanism for implementing the corrections when it involves several different commands or organizations. Naval Aviation places such a premium on the thorough investigation of a mishap that the data and facts gathered in such an investigation fall under the concept of "privileged information" (for class 'C' mishaps and greater). Privileged information collected as a result of a class 'C' or greater mishap investigation cannot be used for punitive purposes against any individual. This concept promotes more openness among investigation witnesses so that the true causes of a mishap can be determined. The results of these investigations are maintained by the Naval Safety Center that makes possible various kinds of statistical analysis of the determined causes of mishaps. This provides an indispensable knowledge base from which commands may use during the ORM process to improve their safety performance.

Computer Network Defense (CND) can benefit from a similar knowledge base of the causes of successful and near-successful IA attacks. Investigations modeled after those conducted for safety mishaps can be used and the results maintained by the Fleet Information Warfare Center (FIWC). FIWC's assignment as the Naval Computer Incident Response Team (NAVCIRT) makes it readily suited to establishing such a knowledge base. The sanitized results of the investigations can be promulgated to all pertinent commands along with the needed corrective actions. The concept of privilege may even be applied to the investigations if some previously agreed to threshold of damage from the incident is exceeded. The establishment of a knowledge base and promulgation of the causes and corrective actions to IA attacks can prevent other commands or organizations within the DON from falling victim to the same attacks. This can be particularly useful in the operational environment were rapid personnel turn over inhibits the ability to preserve corporate memory in many commands.

ORM also enjoys widespread implementation throughout the Fleet because each unit has a safety function that is well trained, and can facilitate its practical application at the unit level. To promote the practical implementation of IARM throughout the Fleet, appendix A is offered as an outline to a possible approach to offer more in-depth courses for IT support personnel, system administrators, IT officer specialists, and decision makers.

C. THESIS APPLICATION TO OTHER MILITARY ORGANIZATIONS

ORM is already being implemented throughout the Fleet. This thesis aims to make a connection between the risk management that commands exercise over the hazards that threaten the safety of personnel and equipment, and the computer and people-based vulnerabilities that threaten our information systems and the data it carries. Computer based information systems are deployed through out the Fleet and serve to fill vital functions in the day-to-day activities of many commands. Reliance on these systems will only continue to increase.

While the NMCI is intended to cover the vast majority of the DON's shore-based information service requirements, it does not extend to our embarked commands and ships. These units can use the IARM process to:

-Improve computer and network security awareness

-Identify assets, vulnerabilities, and controls

-Provide a basis for decisions

-Justify expenditures for security

IARM forces a systematic study of the vulnerabilities in an information system (IS). Security requirements often make an IS more costly to manage, less convenient for users, and function at less than optimal performance capability. IARM can aid decision makers in deciding how much security is right for their systems and justify those penalties that security often produces.

The discussion generated over risk management can improve the security awareness of users, IT support personnel and decision makers alike, thus aiding in complying with OPNAVINST 5239.1B, "Navy Information Assurance Program." It can serve to make everyone knowledgeable of the unit's and DON's security policies, the risks and potential losses that could be experienced by not following those policies, and identify where more training may be needed. By each individual applying the principles of IARM at their level, they can bring unacceptable risks to the attention of the chain of command.

D. FUTURE AREAS OF STUDY

While researching this thesis, the author discovered other subjects that would be excellent topics for future thesis research. These include:

- A thorough look into the Navy's network security policies in light of new technologies (e.g., VPNs), and the manner in which they are written from an organizational-behavior perspective. Poor policy is often the root cause of network security breaches. A recommendation on how policies should be written to be more easily understood, updated and adhered to could be best application of this research.

- Vulnerabilities need to be researched in conjunction with networks and remote access, specifically how to best prevent subversion of remote systems, such as home users. A "honey pot" concept could be used in an attempt to ascertain or update previously unknown methods and types of attacks.
- The use of Intrusion Detection Systems to populate a DON-wide database on the types and frequency of known intrusion attempts on DON computer network systems in order to build a signature-based library of intrusion techniques.
- Inclusion into DON networks of patternless or non-pattern, non-signature based intrusion detection methods when available.
- The development of a structured approach to investigating and documenting successful and near-successful computer network security breaches. The approach can be modeled after the Navy and Marine Corps' Aviation Safety Mishap Investigation (MIRs) and Hazard (HAZREPs) Reporting system.
- The development of a program or course of study to certify decision makers as qualified to accept the risk over decisions concerning computer network and other information systems. A track similar to the SANS Institute GIAC certification process can be developed.
- The development of an online scenario-based test to maintain information assurance awareness among all DON personnel, possibly tailored to different levels of users.

E. FINAL COMMENTS

This final section is dedicated to some observations from the author, his advisors and a fellow student. When ORM was first introduced into the Fleet, it was met with much skepticism as being another Navy program that would require some amount of administration to comply with its mandates. Fortunately, in practice, that did not materialize. The author was fortunate enough to have served with a very talented aviator, graduate of the Navy's Test Pilot School (TPS), he was the Executive Officer (XO) in my last squadron. As the Safety Officer, I was looking for practical ways to implement ORM into our squadron's pre-flight briefings. My XO conveyed to me how it was used when he was a student at TPS. He was a proponent of a structured approach to examine the hazards that we as aviators face during every mission, regardless of the mission's level of difficulty. The outcome was that a short section of each brief would be dedicated to a *discussion* on the potential hazards that might be encountered on the mission and on the controls that the participants would use to manage the risk those hazards posed. The Commanding Officer *vocally* endorsed this approach. Before long, all the aviators of the squadron realized we were just vocalizing a common sense approach to doing our jobs more safely. The ultimate result was that those short discussions raised safety awareness throughout the squadron and allowed the junior aviators to learn from the experiences of the senior aviators in an environment other than the Officer's club! The author hopes that IARM can facilitate a similar paradigm shift in the area of information assurance.

Risk analysis, in general, has been criticized for many reasons. Many risk analysis methods require assigning dollar amounts to assets. This can be difficult, especially when your assets are intangibles like, data, reputation and proprietary knowledge. These dollar values also lead to a false sense of precision or security. The important aspect of these values is the relative size each holds against the other. The differences indicate where controls should first be placed and where further analysis warranted. Finally, once a risk analysis is done, it is usually filed away and forgotten, or is used again a year later. Ideally, risk analysis should be conducted whenever conditions change. (Pfleeger, pp. 470-471) This is a good argument for incorporating IARM as a continuous risk analysis process.

A fellow student working on his thesis concerning VPN implementations observed that, "too many people are too concerned with bit length of keys and implementations of PPTP, and not enough about what is the *value of the data* that is trying to be protected." IARM is a process to deal with exactly this kind of question. The IARM process can aid in facilitating a determination on exactly what needs to be protected and the most efficient way to go about it.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. PROPOSED INFORMATION ASSURANCE RISK MANAGEMENT (IARM) CURRICULA

The Naval Postgraduate School (NPS) has many areas of academic excellence that can be brought together to promote IA in the DON. The Center for Information Systems Security Studies and Research (CISR) is already an acknowledged center of excellence in the field of computer security. The Center for Executive Education (CEE) holds Flag-level seminars on revolutionary business practices and enjoys an excellent reputation among the senior leadership of the Navy. The Information Warfare systems engineering curriculum is active in developing different taxonomies of Information Operations (IO). IA can most benefit from a multi-disciplinary approach that includes computer science, information technology management, organizational behavior and Information Operations. These areas of study can be combined into an "Institute for Information Superiority (IIS)." This center can study how information has become the center of gravity for many functions in today's world and the future. From business commerce to military operations, information, and its unhampered distribution, is seen as the key competitive edge needed to gain the advantage in many confrontational and competitive situations. How that information is managed, protected and distributed can be the focus of such a center. Also, similar to the U.S. Navy and U.S. Marine Corps School of Aviation Safety and the Naval Safety Center and their positions as the standard-bearers, developers and promoters of ORM throughout the Fleet, the IIS can easily assume the same position vis-à-vis IARM.

One of the key reasons ORM has been adopted throughout the Fleet is because senior decision makers have been convinced of its applicability and utility in preventing mishaps. With its established credibility and reputation, NPS can have tremendous influence over those same decision makers DOD wide. NPS can leverage this advantage by offering a weeklong, executive level course to senior decision makers (O-5 and above, and GS equivalent) on information assurance and its importance to the DON mission. This course would introduce the basics of information assurance and the critical role decision makers play in managing the risks associated with our computer networks. It would have at its core the IARM process. This course could use the same philosophical approach as the Aviation Safety School's six-day Aviation Safety Commander (ASC) course offered to unit Commanding Officers, Officers-in-Charge, and Safety Officers of major commands. An NPS executive level course can be instrumental in raising awareness of network security and IA issues and the concepts of IARM given our increased reliance on computer networks and the information it carries. It may also facilitate meeting the Presidential Decision Directive 63 (PDD-63) requirement to improve the security capabilities of our nation's cyber-based critical infrastructure, and thus be applicable DOD wide.

ORM enjoys widespread implementation throughout the Fleet because each unit has a safety function that is well trained, and can facilitate its practical application at the unit level. To promote the practical implementation of IARM throughout the Fleet, the IIS can also offer a more in-depth course for senior IT support personnel and those individuals assigned with network security duties. This course could emulate the approach that the Aviation Safety School uses with its 28 instructional-day course for unit Aviation Safety Officers. This IT support personnel/information systems security officer (ISSO) course can be tailored to focus on officer IT specialist and enlisted IT support corps. This advanced course can be divided into the following areas, much like the SANS Institute uses during its conferences:

-Fundamentals of Information Assurance

-Firewalls and Perimeter Protection

-Intrusion Detection Systems

-Incident Handling

-Current High-Threat Vulnerabilities and Cracker Exploits

-Effective Audit and Vulnerability Assessment

-IARM

The above two courses can be offered in cooperation with other DOD, government, academic or civilian institutions (e.g., SANS Institute, Carnegie Mellon, National Security Agency (NSA), Fleet Information Warfare Center (FIWC), etc.) and tailored to the needs of the participants if warranted. Classified portions of the above courses can also be offered as NPS has the required facilities to do this, and would make the executive level course more worthwhile for busy senior decision makers.

It is recognized that there are other entities endeavoring to accomplish these ends, but a more coordinated effort will gain efficiencies where none exist now. NPS is uniquely positioned to straddle the boundaries between the military, government, academia and industry to realize these efficiencies. The NPS IIS can ultimately serve as the center for DON's efforts to improve IA throughout the Fleet, and possibly throughout the Federal Government.

The Naval Postgraduate School (NPS) can test some of the concepts above by first introducing them into the Information Strategy and Operations (ISO) curriculum.

The purpose of the ISO curriculum is to "develop a cadre of Unrestricted Line (URL) Officers with the expertise to innovatively create concepts of war fighting and the application of information technology (IT) to implement them operationally." This cadre would benefit greatly from a thorough understanding of being able to apply the principles of ORM to IA (i.e., IARM) because they are the ones expected to facilitate the integration of IT into all the Navy does operationally.

The following is offered as a possible outline of IA curricula that can be applied to four target groups: Line officers, IT officer corps, enlisted IT support corps, and general users, and emulates closely the approach taken to implement ORM throughout the fleet. The note slides in appendix B is offered as the basis for an indoctrination presentation for IARM.

A. INDOCTRINATION TRAINING OUTLINE

Audience: All Users

The purpose of this curriculum is to provide a basic understanding of what IA is, what risk management is, the benefits derived from it, the concepts that apply to it, and how to do time critical IARM. Content:

- IARM terms and definitions
- IARM introduction concept
- Four principles of IARM
- IARM vs. traditional approach
- Benefits of IARM
- Three levels of IARM

- Time critical IARM, examples and demonstrations
- Specific applications (demonstrating applicability to existing IA processes and procedures)

Appendix B is offered as a possible presentation for this course

B. USER OUTLINE

Audience: Junior IT Support Personnel

This curriculum is applicable to all users who use IT as a vital portion of their everyday duties, and the more junior members of the IT support corps referred to below, with the purpose of expanding their understanding of IA and the deliberate five-step process of IARM. Content: Indoctrination Training plus:

- Fundamentals of Information Assurance (IA)
- Deliberate IARM process and demonstration
- Basic vulnerability identification, tools, examples
- Vulnerability assessment tools and examples
- Risk assessment tools and examples
- Deliberate IARM practical exercise
- Specific applications (demonstrating applicability to existing IA processes and procedures)

C. INFORMATION TECHNOLOGY SUPPORT CORPS OUTLINE

Audience: Experienced IT Support Personnel and System Administrators

This curriculum is applicable to those more senior who actually maintain, support and administrate information systems within their commands with the purpose of expanding their understanding of current threats and vulnerabilities, and provide the tools necessary for implementing IARM in their command. Content: Users curriculum plus:

- Advanced Information Assurance
- Firewalls and Perimeter Protection
- Intrusion Detection Systems
- Incident Handling
- Current High-Threat Vulnerabilities and Cracker Exploits
- Basics of effective Audit and Vulnerability Assessment
- In-depth vulnerability identification tools and examples
- Risk assessment tools and examples (cross section of available tools)
- Command implementation and leadership concepts
- Specific application (demonstrating applicability to existing IA processes and procedures)

D. INFORMATION TECHNOLOGY (IT) OFFICER CORPS OUTLINE

Audience: IT Officer Specialist

This curriculum is applicable to those officers who are the enablers of the integration of IT into the everyday activities that are performed in the DON with the purpose to give enough knowledge to understand in-depth and deliberate IARM, what

IARM can provide, and how to implement it within their units. Contents: IT Support Corps curriculum plus:

- Introduction to Information Operations (IO)/Information Warfare (IW)
- Advanced studies on the current threats and vulnerabilities
- Specific applications

E. SENIOR LEADERSHIP OUTLINE

Audience: O-5 and Above (GS equivalent)

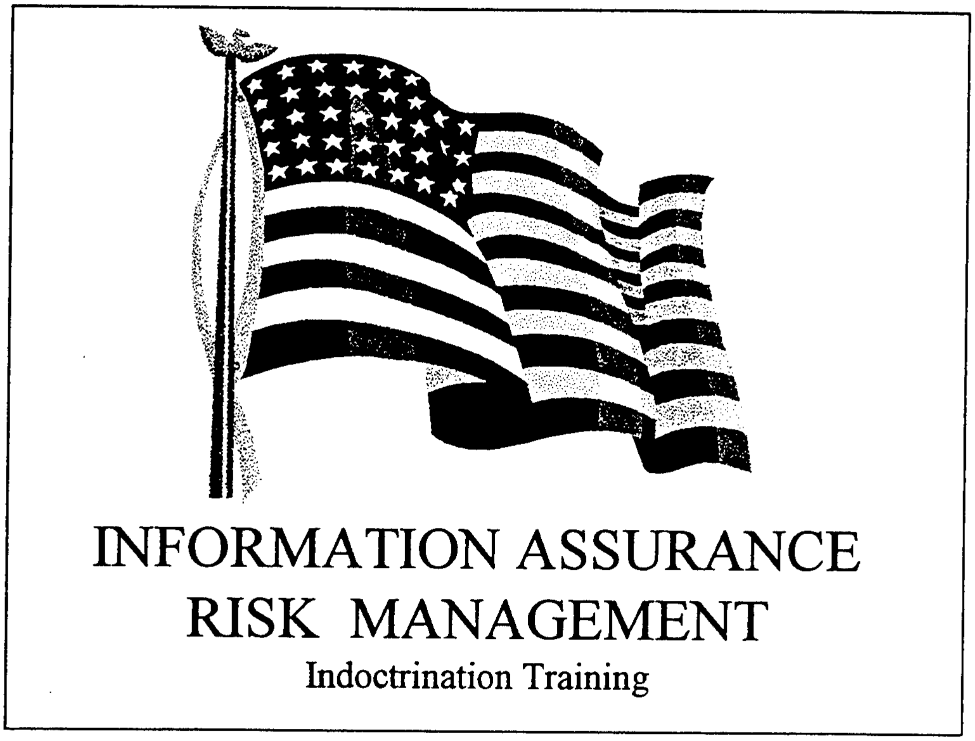
This curriculum is applicable to the senior leadership in the DON who will make IARM implementation effective through control of the rewards system used in the DON, with the purpose to provide a basic understanding of the IARM process, the benefits derived from it, the three levels and some of the applications of IARM. Content:

- IA background
- Current threats and recent exploitations (classified if necessary)
- Three levels of IARM
- Five step process of IARM
- IARM vs. traditional approach
- Specific fleet applications
- Benefits of IARM

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. POWERPOINT PRESENTATION NOTE SLIDES

Information Assurance Risk Management (IARM) Indoctrination Presentation



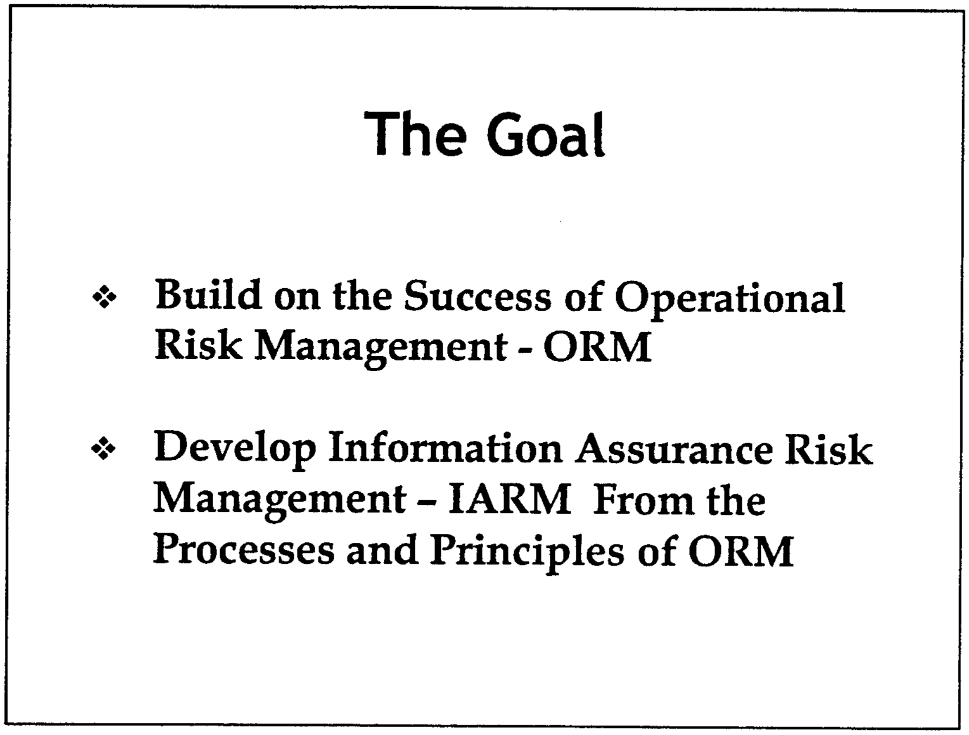
INFORMATION ASSURANCE RISK MANAGEMENT

Indoctrination Training

You've all practiced Risk Management during your careers, or you wouldn't be here. However, the risk posed to our information and data are significant. We here accounts everyday how civilian and DOD systems are being hacked and major commerce sites being brought down. With our going to the NMCI, and working on ways to tactically take advantage of information systems, like in Network Centric Warfare. The need for effective Computer Network Defense (CND) becomes readily apparent.

Information Assurance Risk Management doesn't just improve security awareness, but it improves our ability to accomplish our mission efficiently and effectively.

The introductory training which follows is designed to give the audience a basic understanding of IARM. Everyone in the command, from the most junior person to the CO, should receive introductory training.



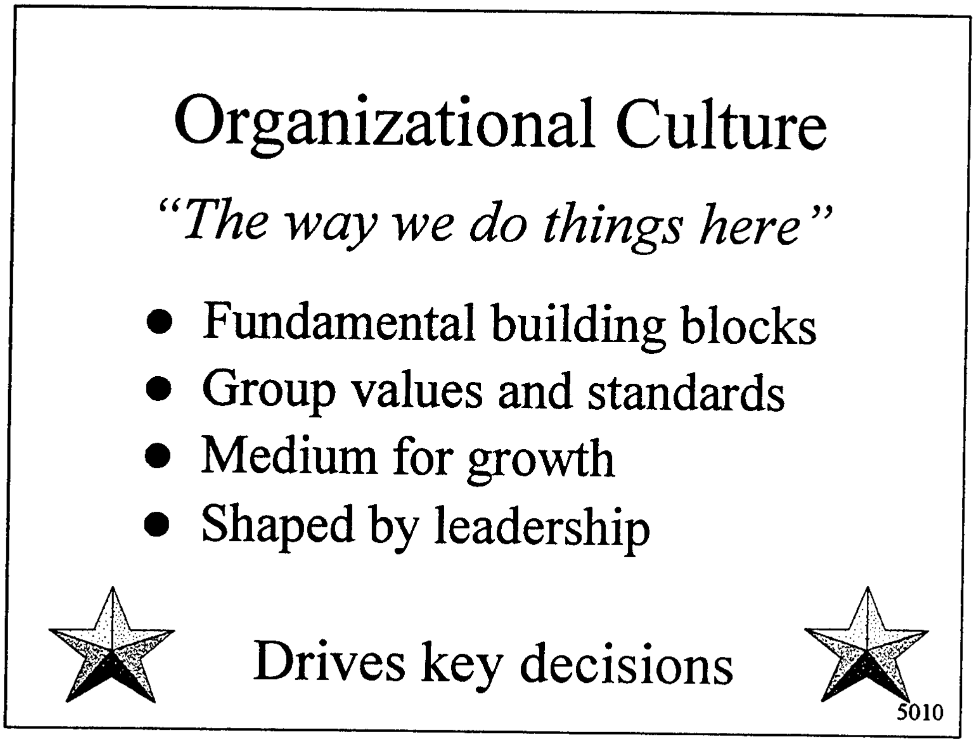
The Goal

- ❖ Build on the Success of Operational Risk Management - ORM
- ❖ Develop Information Assurance Risk Management – IARM From the Processes and Principles of ORM

Begin with:

Information Assurance Risk Management (IARM) is a form of Operational Risk Management (ORM). ORM has and is used to improve safety throughout the Fleet. In the same way IARM can be used to improve Computer Network Defense (CND) by developing effective Information Assurance (IA) practices and raising overall security awareness.

We'll discuss the origin and basics of ORM, then apply it to the area of IA. Lastly. We'll finish with an overview of the IARM process.



Organizational Culture

"The way we do things here"

- Fundamental building blocks
- Group values and standards
- Medium for growth
- Shaped by leadership

Drives key decisions

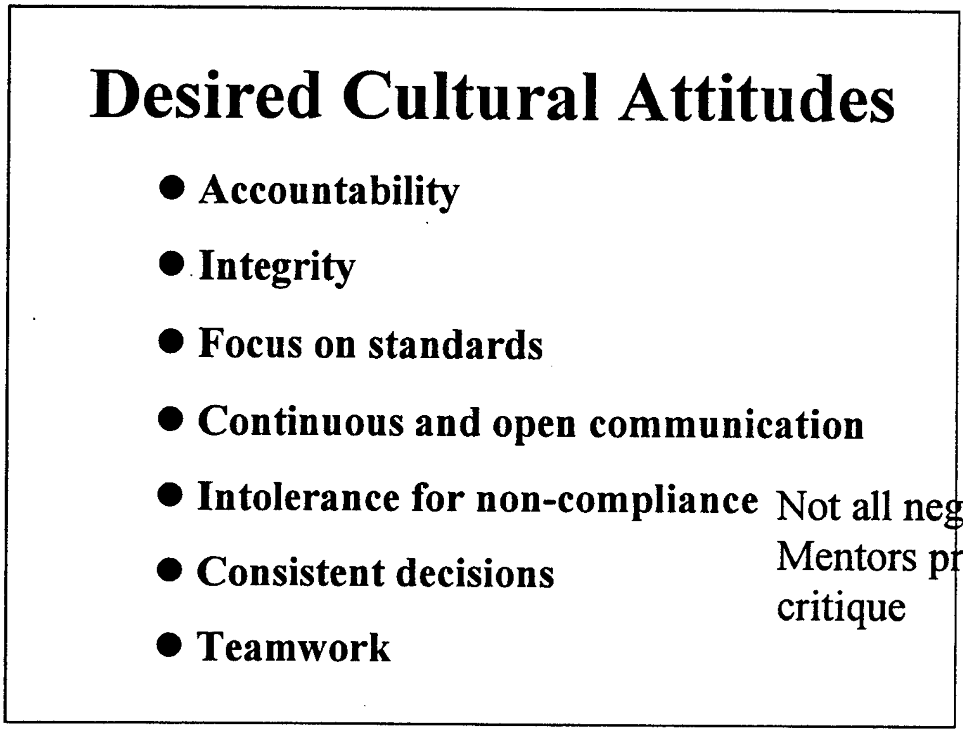
5010

ORM is designed to change culture. It strives to change the way we perform everyday tasks, and that's not easy!

How do we change people's attitudes and actions???

Good Organizational Culture requires a visionary leader, enhances people development, requires straight talk, mandates that you hire/fire the right people, and demands accountability – no act goes unnoticed.

What is the Outcome from a good organizational culture?



Desired Cultural Attitudes

- **Accountability**
- **Integrity**
- **Focus on standards**
- **Continuous and open communication**
- **Intolerance for non-compliance**
- **Consistent decisions**
- **Teamwork**

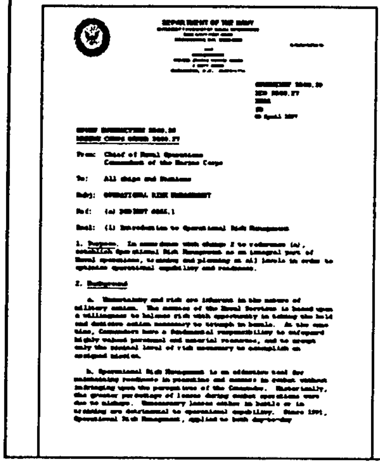
Not all negative.
Mentors professional
critique

HOW DO WE ... IMPROVE THE ...- **Organization**
- Culture
- Process

As we are beginning to see, theses attributes just don't apply to present activities, but all activities we do in the Navy.

ORM GUIDANCE

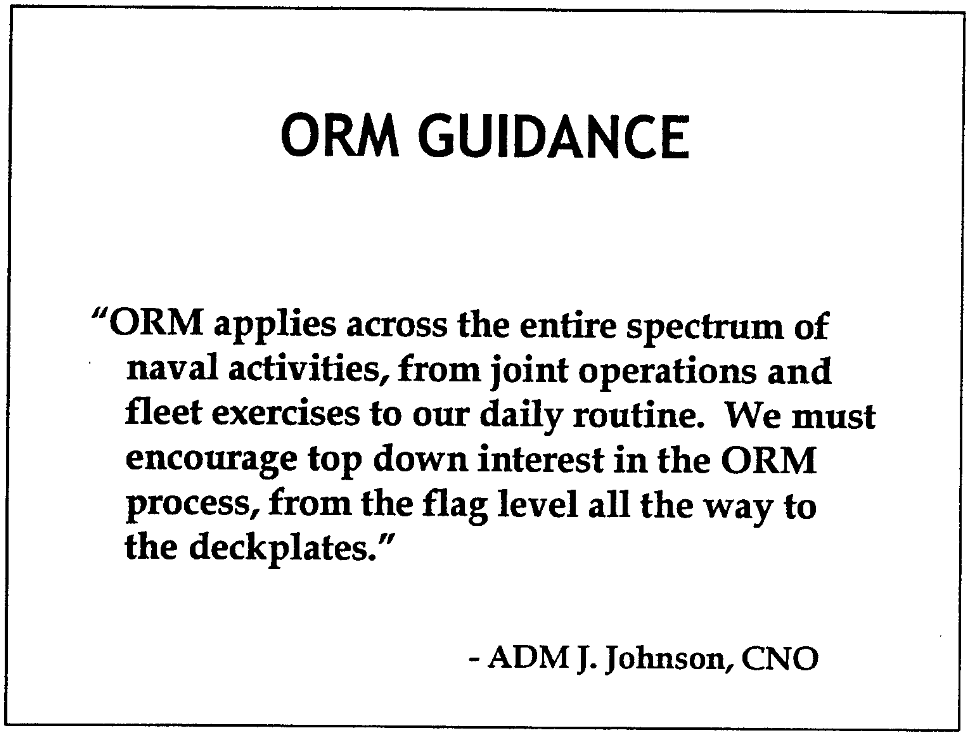
OPNAVINST 3500.39



CO's should ensure ORM is implemented into all levels of the command. Examples include, but are not limited to:

- **Train all personnel on ORM process.**
- **Incorporate identified hazards, assessments & controls into briefs, notices, and written plans.**
- **Conduct thorough risk assessments for all new or complex evolutions, defining acceptable risk and possible contingencies for the evolution.**

As the instructions directs, ORM applies to all activities, both on and off duty! It is a people-focused procedure to facilitate a change in the way we view our everyday activities

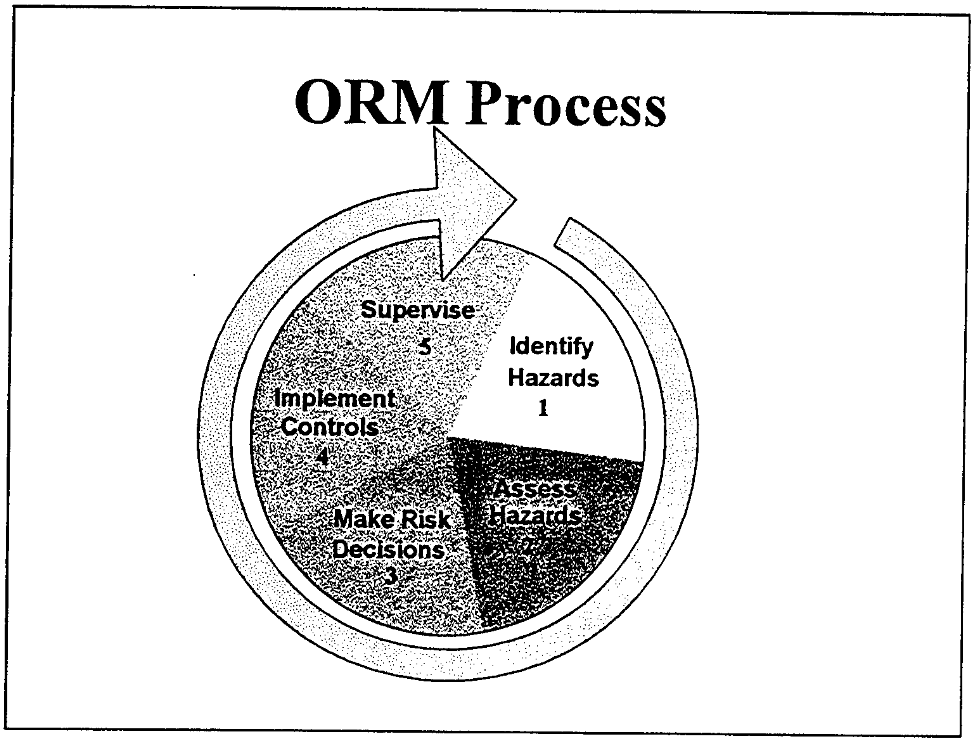


ORM GUIDANCE

"ORM applies across the entire spectrum of naval activities, from joint operations and fleet exercises to our daily routine. We must encourage top down interest in the ORM process, from the flag level all the way to the deckplates."

- ADM J. Johnson, CNO

Read the former CNO's quote. Note that the present CNO, ADM Clark, is also a supporter.



ORM Process

Identify Hazards 1

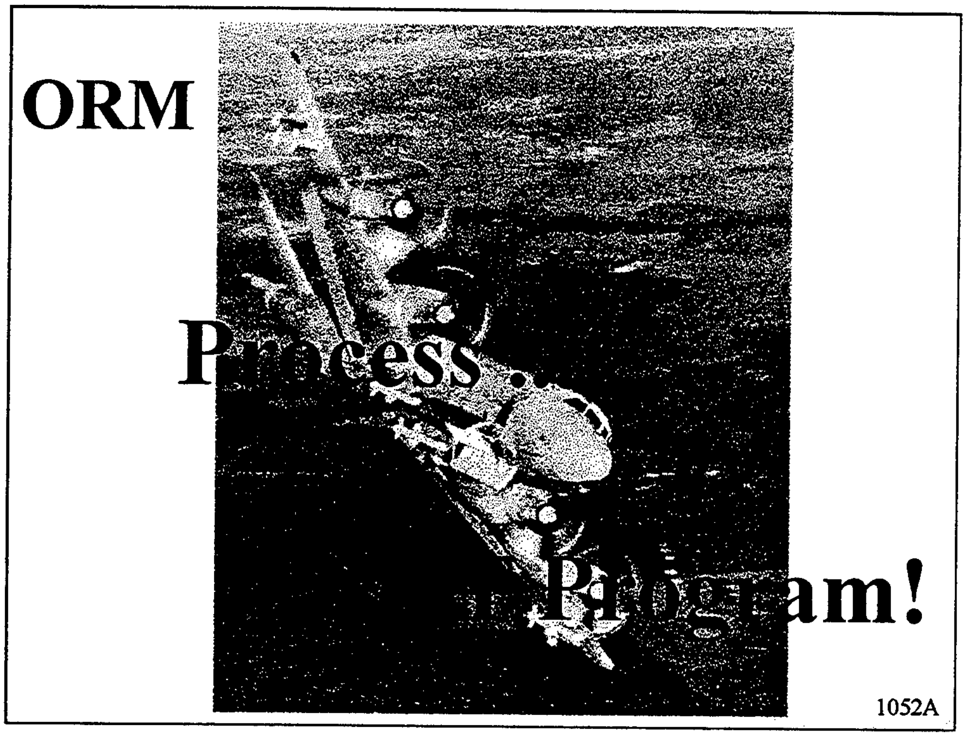
Assess Hazards 2

Make Risk Decisions 3

Implement Controls 4

Supervise 5

Here is depicted the 5 steps of ORM in a pie diagram to help you visualize where we are going before we begin the IARM process. Note that it is a continuous process when applied correctly.



ORM

Process .

Program!

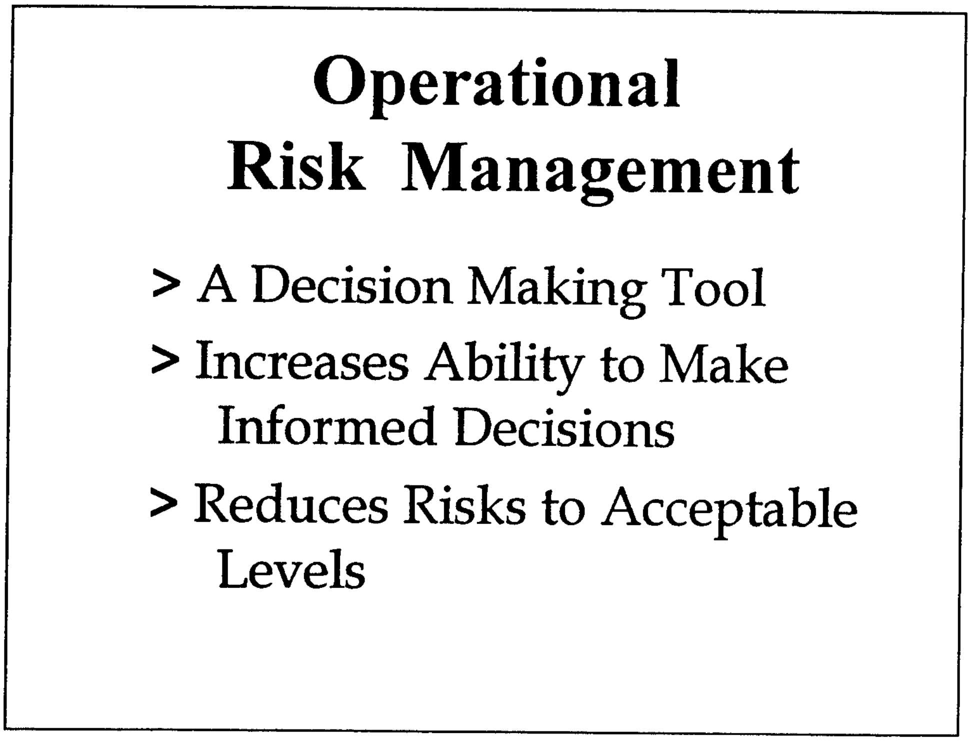
1052A

ORM is a PROCESS, lust like we will show IARM to be a process. This <u>is not</u> a new program to be added to inspection checklists.

Risk Management will eventually become a way of life to each individuals way of thinking.

The CMC/CNO ORM instruction calls for no additional administrative burden and the same applies to IARM.

The speaker may corroborate this aspect of ORM through any personal, first hand experience. In any case, it needs to be stressed as an important aspect of ORM.



Operational Risk Management

- > A Decision Making Tool
- > Increases Ability to Make Informed Decisions
- > Reduces Risks to Acceptable Levels

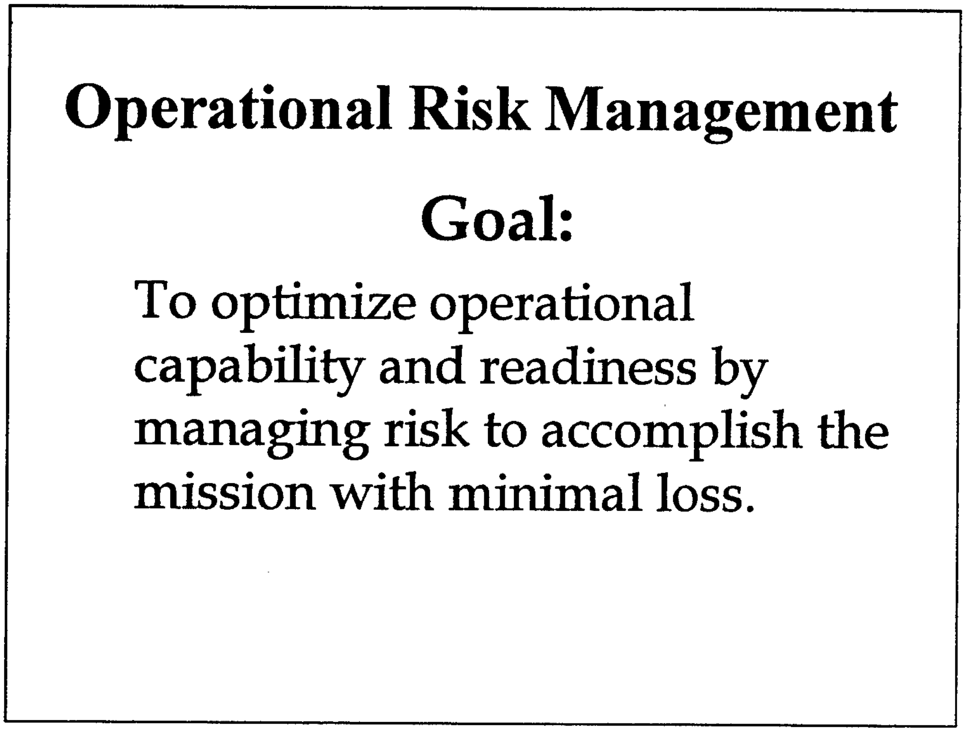
The ORM process:

- is a decision making tool which can be used by people at all levels to increase operational effectiveness.

- increases the ability to make informed decisions by providing the best baseline of knowledge and experience available.

- minimizes risks to acceptable levels by systematically applying controls to each risk which is not acceptable. The amount of risk we will take in war is much greater than that we should be willing to take in peace, but the same systematic process should be used to evaluate risks in both situations.

Many you now be making a connection between the relationship of ORM and safety, and the similar relationship between IARM and security.

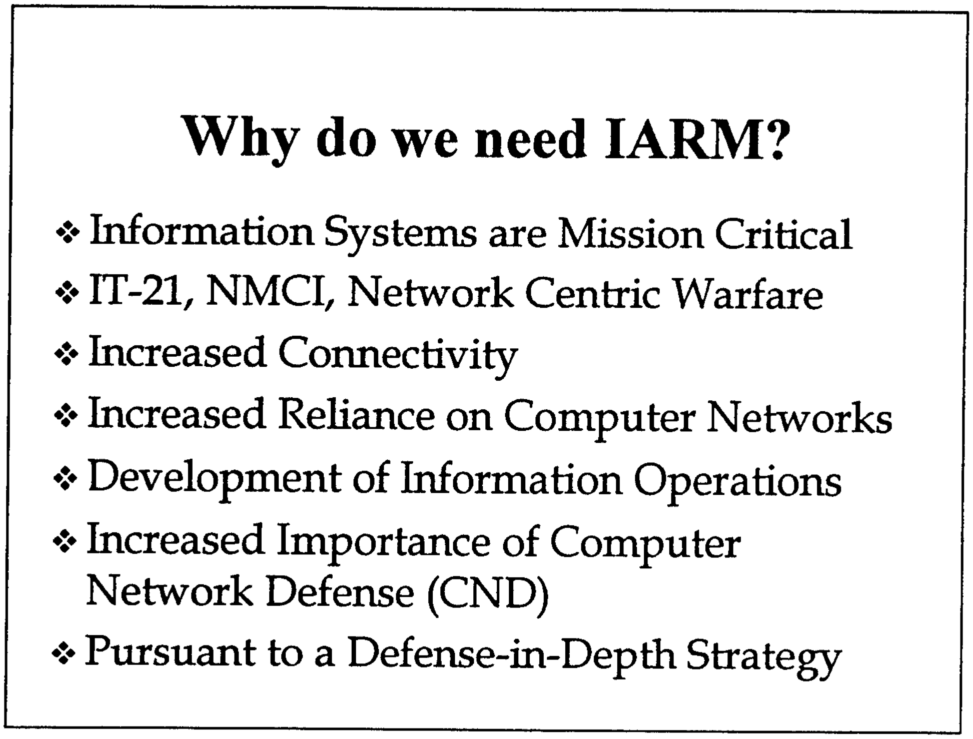


Operational Risk Management

Goal:

To optimize operational capability and readiness by managing risk to accomplish the mission with minimal loss.

Obviously, we can't eliminate risk in our everyday activities, but we can reduce the amount of loss we experience (in data loss and compromise, equipment and mission accomplishment).



Why do we need IARM?

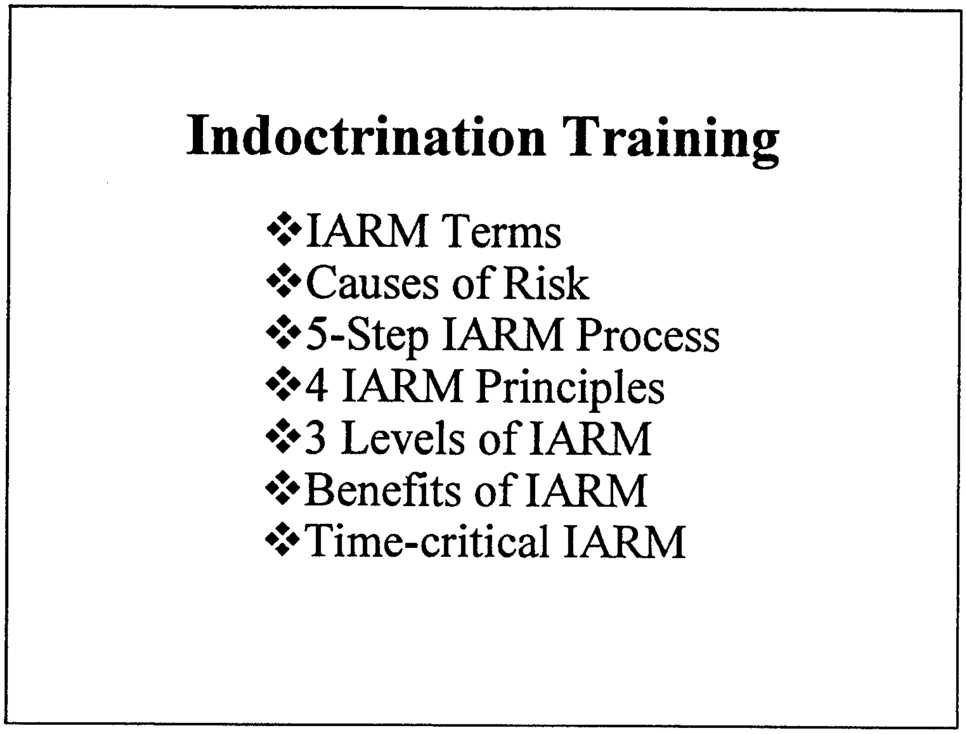
- ❖ Information Systems are Mission Critical
- ❖ IT-21, NMCI, Network Centric Warfare
- ❖ Increased Connectivity
- ❖ Increased Reliance on Computer Networks
- ❖ Development of Information Operations
- ❖ Increased Importance of Computer Network Defense (CND)
- ❖ Pursuant to a Defense-in-Depth Strategy

From the NMCI Information Security fact sheet:

"With the significant benefits of increasing network connectivity comes a corresponding increase in the potential for detrimental information warfare (IW) attacks and physical threats from natural and man-made disasters. As modern warfare becomes more dependent on information technology (IT) resources like NMCI services, NMCI network defense must be viewed as a Defensive warfare activity."

The trend for relying on information systems is only increasing!

IARM is Defense-in-Depth for the weak link in computer network and information systems security – the human factor.



Indoctrination Training

❖IARM Terms

❖Causes of Risk

❖5-Step IARM Process

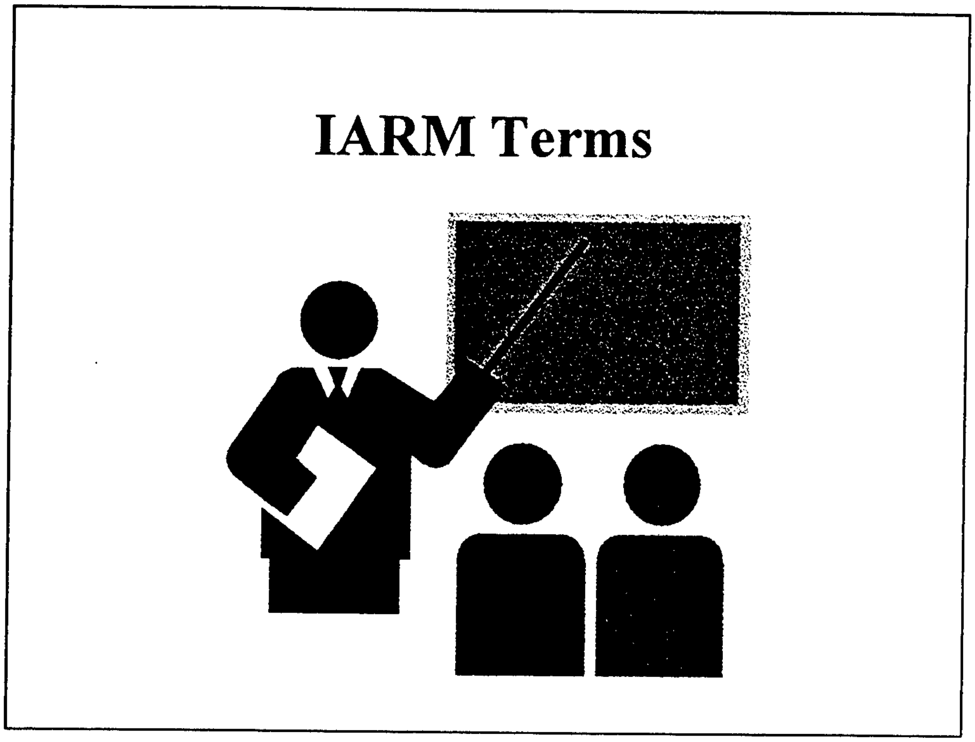
❖4 IARM Principles

❖3 Levels of IARM

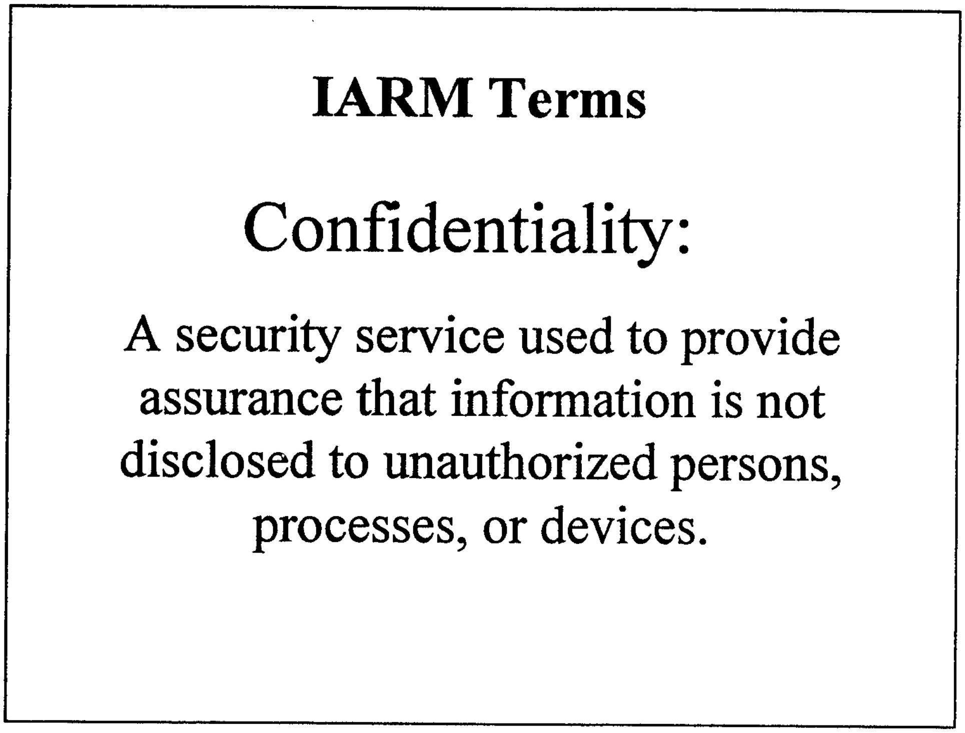
❖Benefits of IARM

❖Time-critical IARM

Here's a summary of what we'll cover in indoctrination training.



IARM Terms



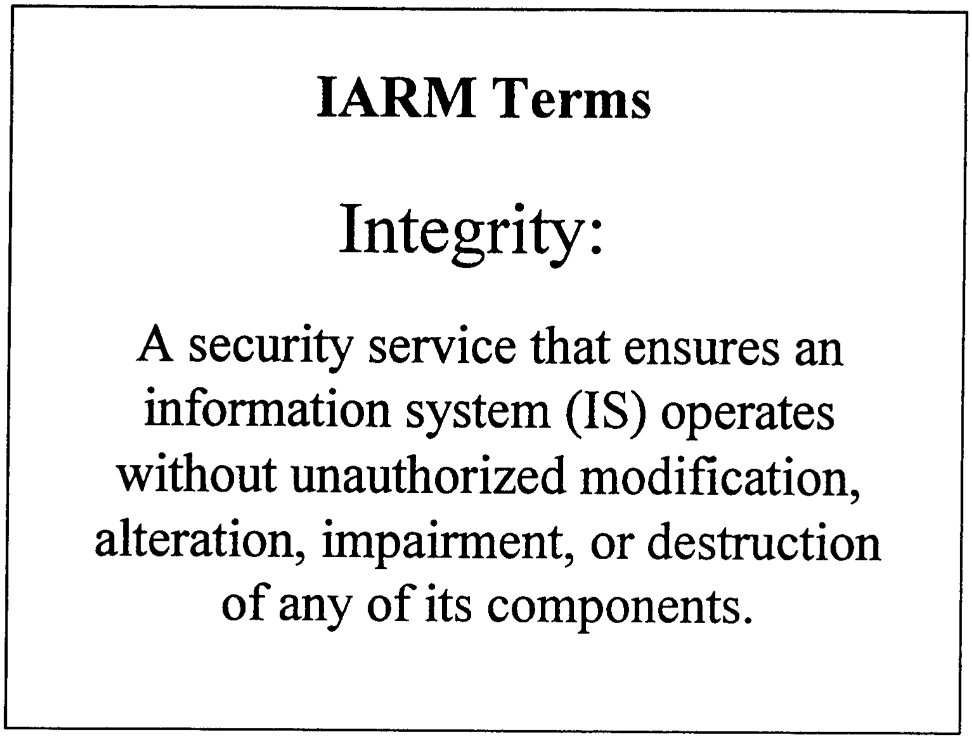
IARM Terms

Confidentiality:

A security service used to provide assurance that information is not disclosed to unauthorized persons, processes, or devices.

Read definition. A security service used to provide assurance that information is not disclosed to unauthorized persons, processes, or devices.

Traffic flow and traffic analysis are examples of threats to confidentiality. Threats to confidentiality are usually characterized as passive as the attacker does not have to give away his/her presence in attempting the attack.

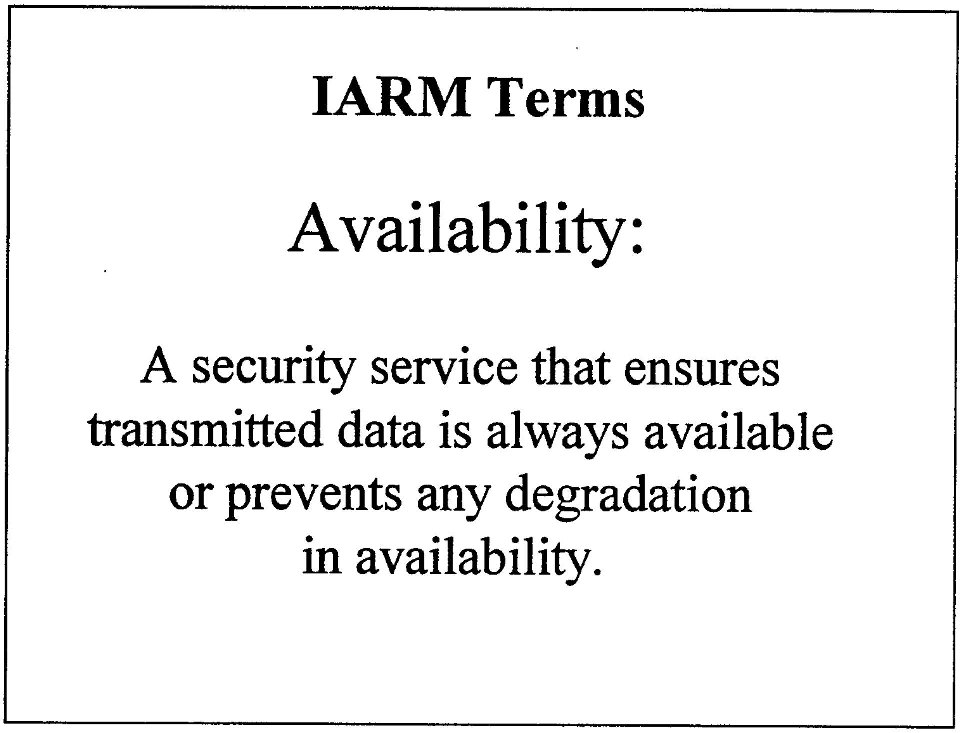


IARM Terms

Integrity:

A security service that ensures an information system (IS) operates without unauthorized modification, alteration, impairment, or destruction of any of its components.

<u>Read definition.</u> A security service that ensures an information system (IS) operates without unauthorized modification, alteration, impairment, or destruction of any of its components.



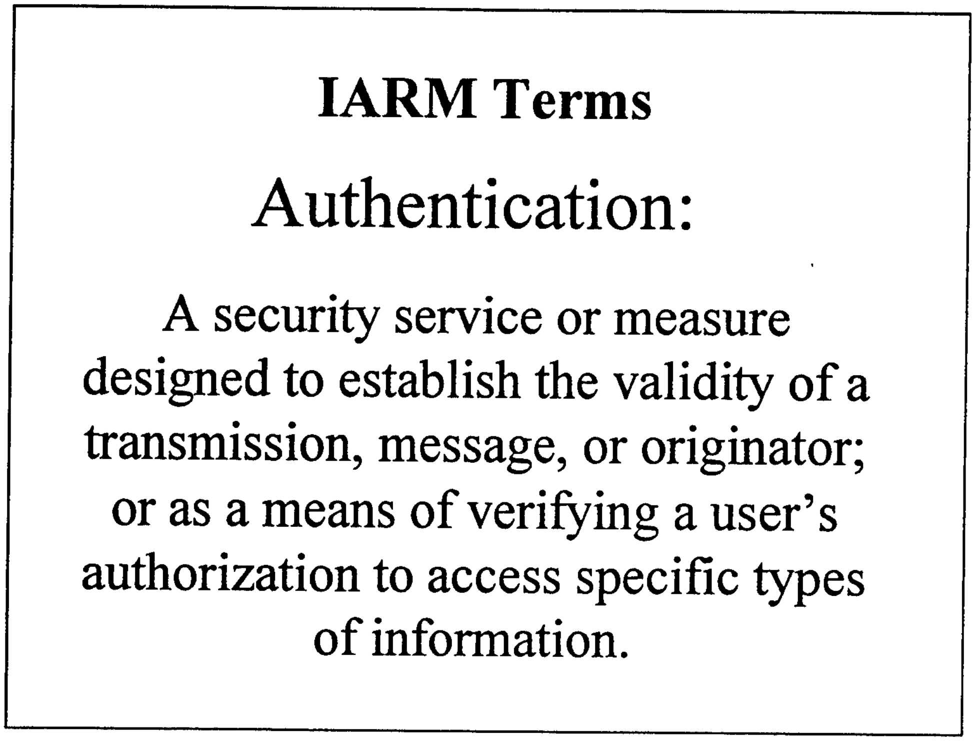
IARM Terms

Availability:

A security service that ensures transmitted data is always available or prevents any degradation in availability.

Read definition. A security service that ensures transmitted data is always available or prevents any degradation in availability.

Some of the network support types might assert that availability is up time divided by total time. That's perfectly correct, but we are trying to frame these terms in an information assurance context. This illustrates a very good point, depending on where your focus is within the functions of an *information system* dictates the type of language used. IARM attempts to get everyone involved with an information system using the same terminology.

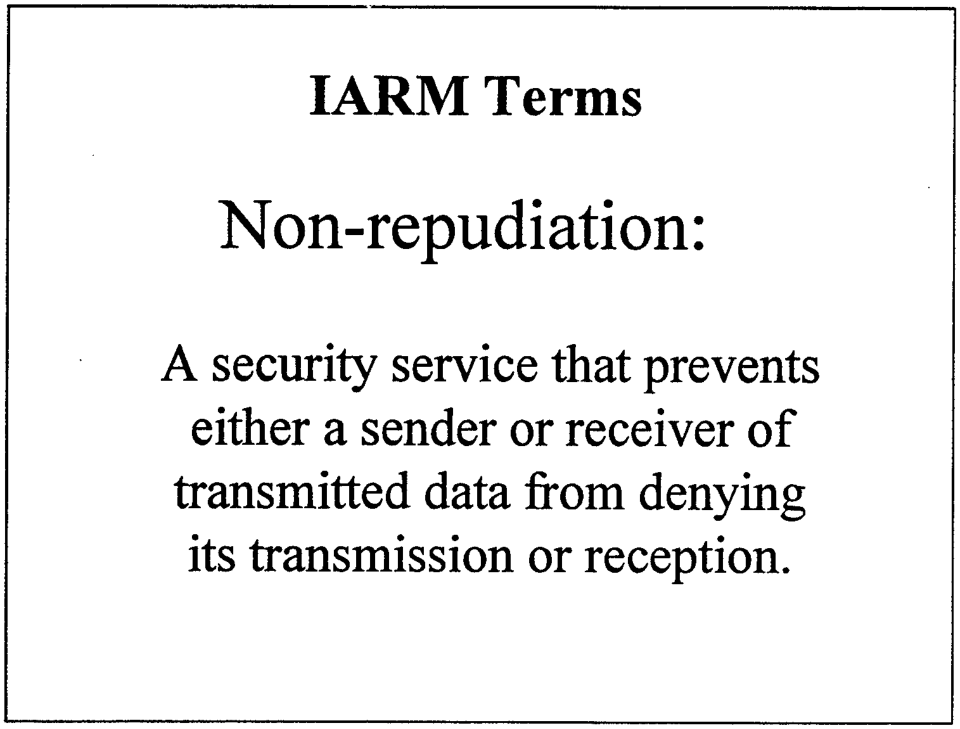


IARM Terms

Authentication:

A security service or measure designed to establish the validity of a transmission, message, or originator; or as a means of verifying a user's authorization to access specific types of information.

Read definition. A security service or measure designed to establish the validity of a transmission, message, or originator; or as a means of verifying a user's authorization to access specific types of information.

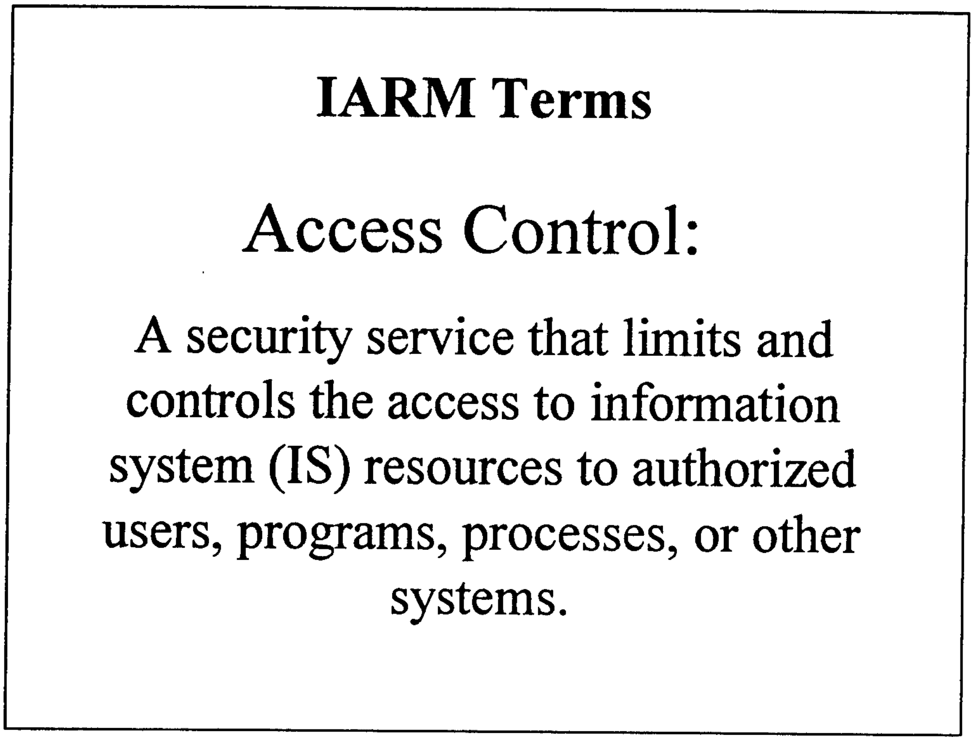


IARM Terms

Non-repudiation:

A security service that prevents either a sender or receiver of transmitted data from denying its transmission or reception.

Read definition. A security service that prevents either a sender or receiver of transmitted data from denying its transmission or reception.



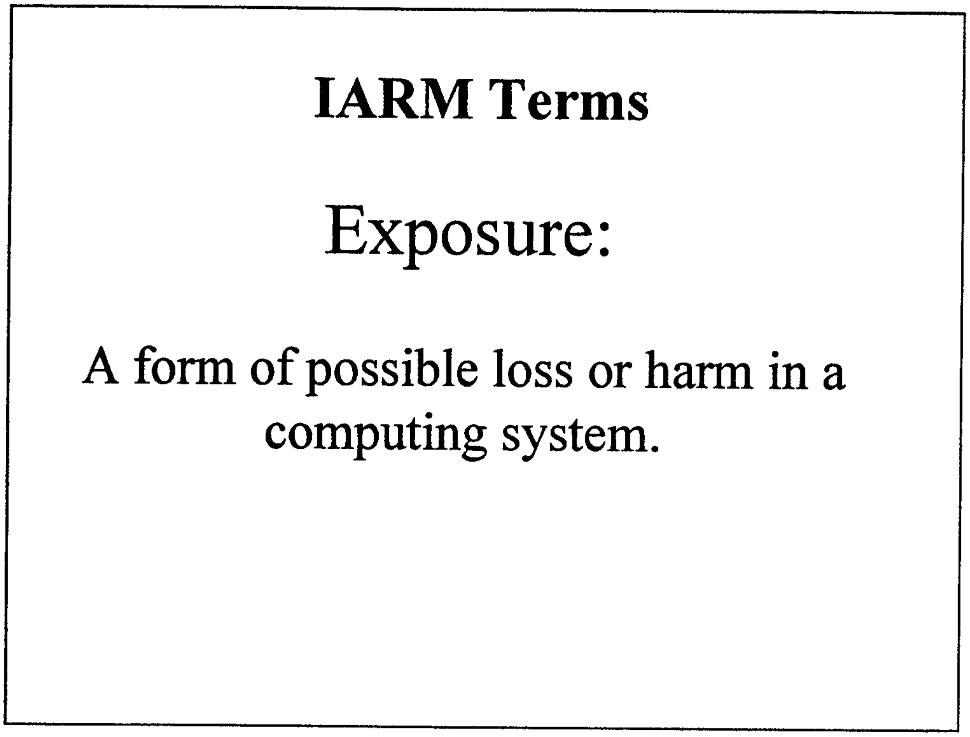
IARM Terms

Access Control:

A security service that limits and controls the access to information system (IS) resources to authorized users, programs, processes, or other systems.

Read definition. A security service that limits and controls the access to information system (IS) resources to authorized users, programs, processes, or other systems.

Note: We are not just talking about the log on window you see when you step up to a WINTEL work station, but the services that control who or what talks to what systems and how.

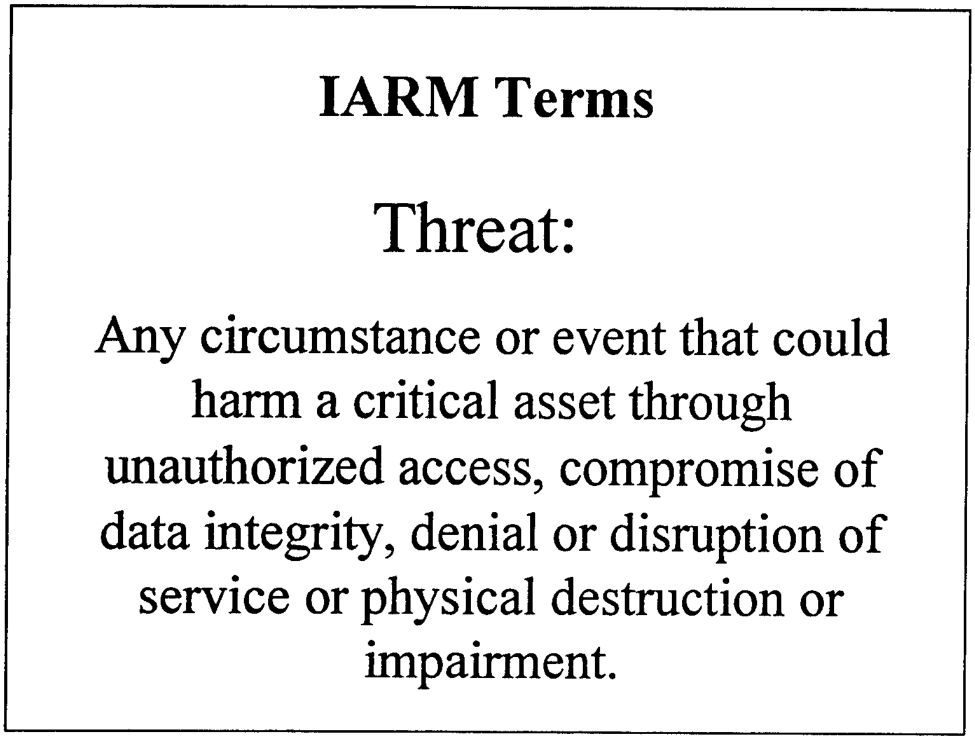


IARM Terms

Exposure:

A form of possible loss or harm in a computing system.

Read definition. A form of possible loss or harm in a computing system.



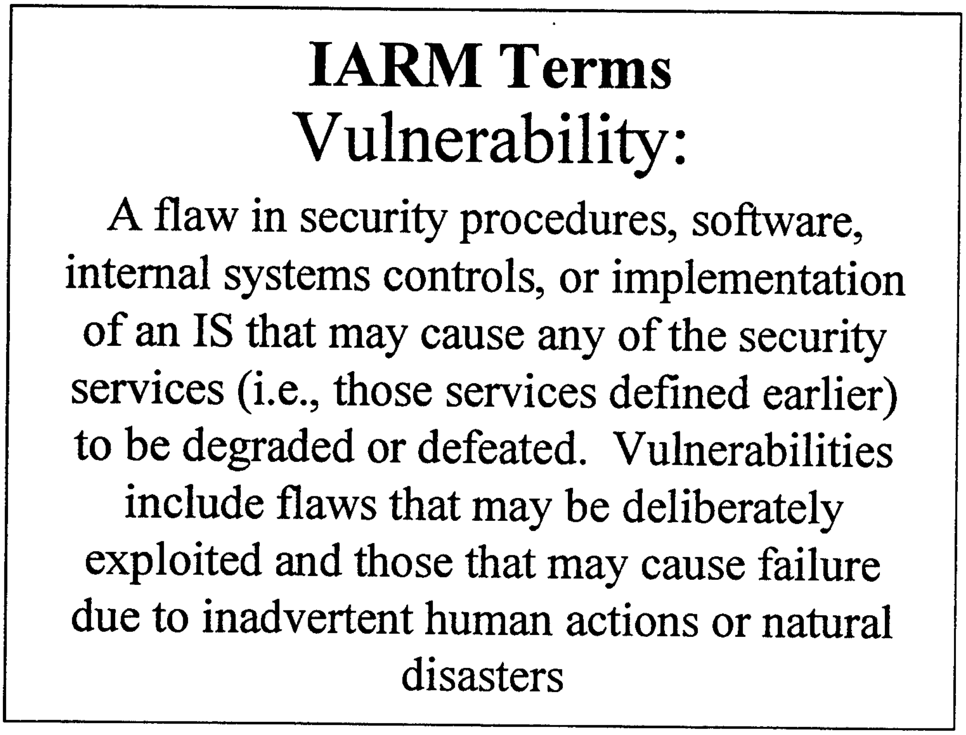
IARM Terms

Threat:

Any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service or physical destruction or impairment.

Read definition. Any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service or physical destruction or impairment.

This can also be any attack that takes advantage of a vulnerability. (e.g., buffer overflow, social engineering, spoofing, eavesdropping, etc.) Flooding or combat damage can be just as potent a threat.



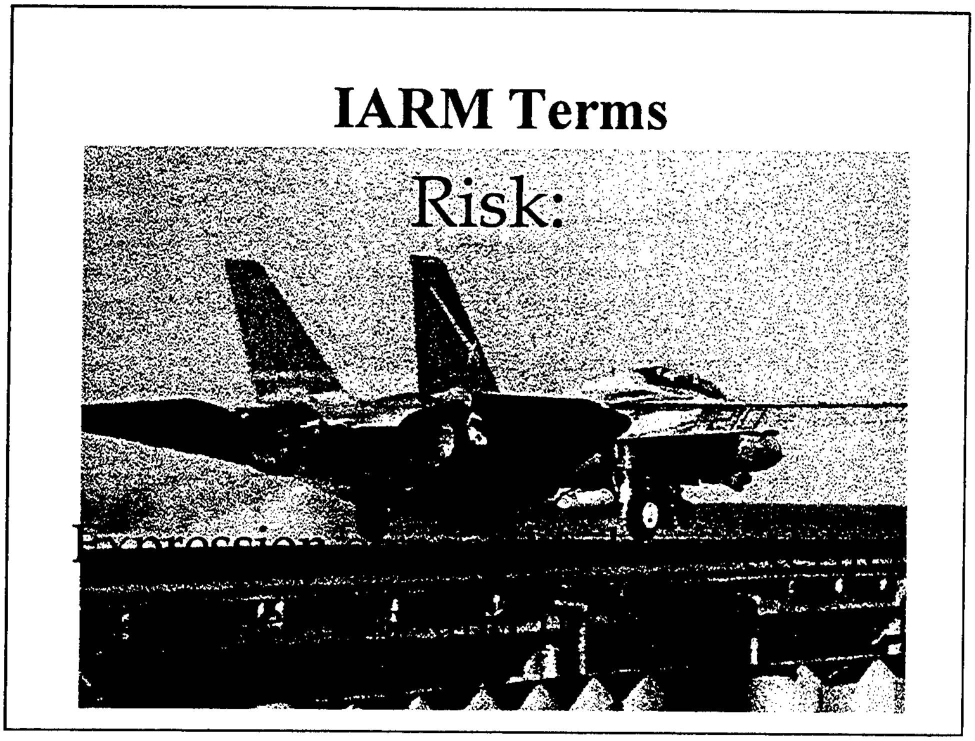
IARM Terms

Vulnerability:

A flaw in security procedures, software, internal systems controls, or implementation of an IS that may cause any of the security services (i.e., those services defined earlier) to be degraded or defeated. Vulnerabilities include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters

Read definition. A flaw in security procedures, software, internal systems controls, or implementation of an IS that may cause any of the security services (i.e., those services defined above) to be degraded or defeated. Vulnerabilities include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters.

Most of us think of data loss or compromise when we think of information systems vulnerabilities. But, remember the last part of this definition...anything which can cause an information systems' security to be degraded is a vulnerability (e.g., Used for Distributed Denial of Service Attacks (DDoS)). That includes enemy threats, security threats, natural threats, inefficient use of assets, training degradation, something which could damage command image and credibility, etc..



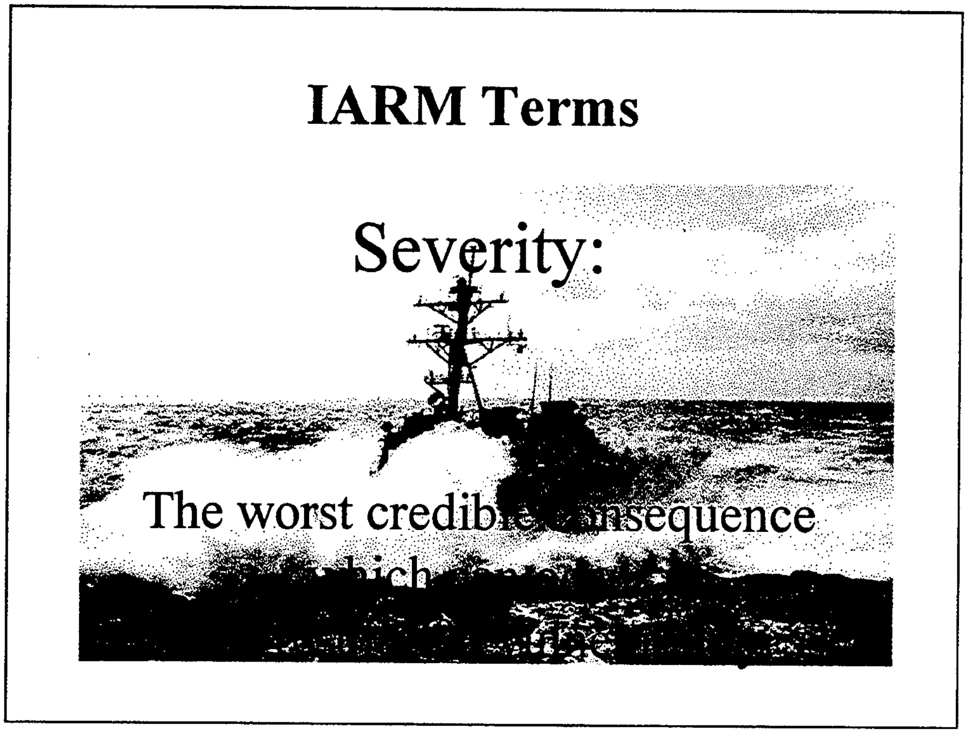
IARM Terms

Risk:

Expression

<u>Read definition</u>. Expression of possible loss in terms of severity and probability.

What do we mean when we say severity and probability?

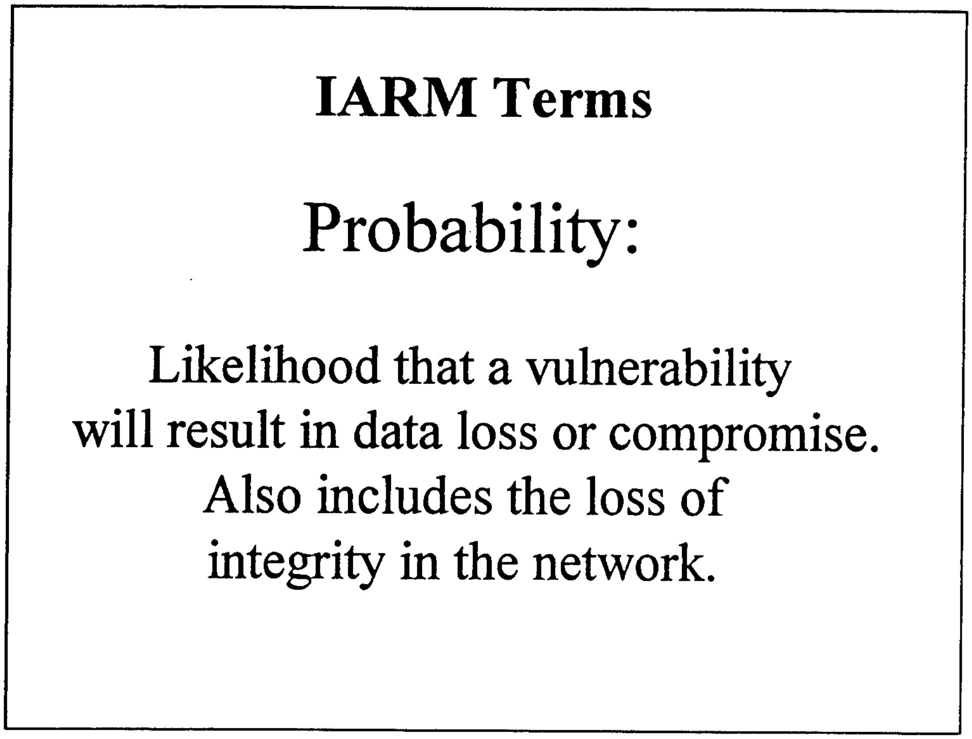


IARM Terms

Severity:

The worst credible consequence which [illegible]

Read definition. For the purposes of IARM, severity is the worst credible consequence which can occur as a result of a vulnerability. It is the potential degree of data loss or compromise. It is an expression of how serious the compromise, how much equipment damage, how much lost time, money, man-hours or credibility could be experienced as a result of the vulnerability.

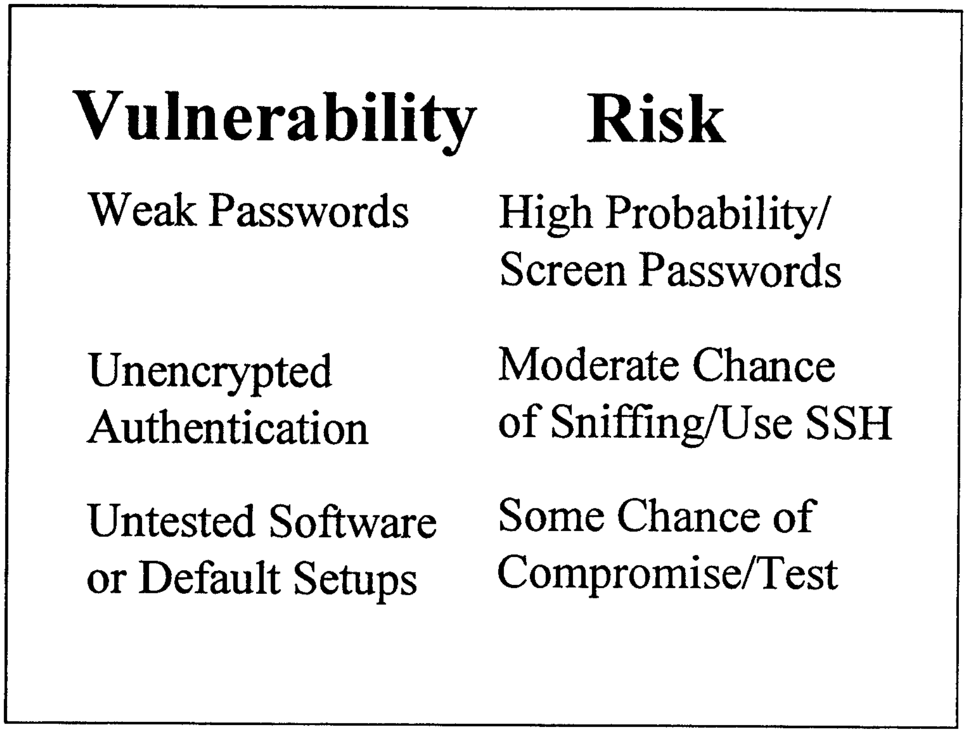


IARM Terms

Probability:

Likelihood that a vulnerability will result in data loss or compromise. Also includes the loss of integrity in the network.

Read definition. The likelihood that a vulnerability will result in data loss or compromise is based on factors such as location, exposure, personnel, experience and historical information.



Vulnerability	Risk
Weak Passwords	High Probability/ Screen Passwords
Unencrypted Authentication	Moderate Chance of Sniffing/Use SSH
Untested Software or Default Setups	Some Chance of Compromise/Test

Discuss the difference between a vulnerability and risk as some may confuse the two. Go back to the vulnerability definition slide if need be.

Weak passwords are a vulnerability. The associated risk is there is a high probability of a successful attack on access control by someone being able to guess the password and gain unauthorized access.

Unencrypted authentication is a vulnerability. The associated risk is that there is a moderate probability of a successful attack on confidentiality by someone sniffing your collision domain and being able to read authentication data.

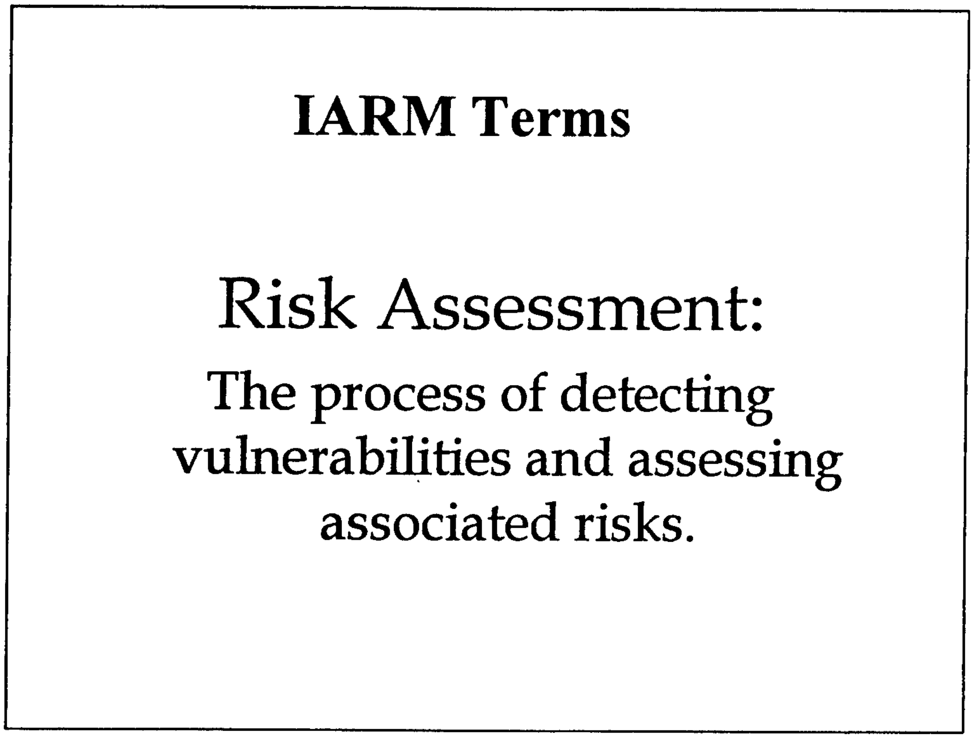
Untested or default setups are a vulnerability. The associated risk is that there is some chance a successful attack on availability as an untested program may have a virus that reformats hard drives, or some chance of a successful attack on access control as not all the security features may be enabled on a default installation.

Note: Some may point out that the vulnerabilities listed above are just the symptoms of true vulnerabilities, which are breaches of a system's security service cited earlier. Recall the definition of a vulnerability:

A flaw in security procedures, software, internal systems controls, or implementation of an IS that may cause any of the security services (i.e., those services defined earlier) to be degraded or defeated. Vulnerabilities include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters.

We are interested in discovering the flaws and symptoms so that the vulnerabilities to our security services can be identified and thus remedied if possible.

Possible remedies are included to aid in the understanding of this slide.



IARM Terms

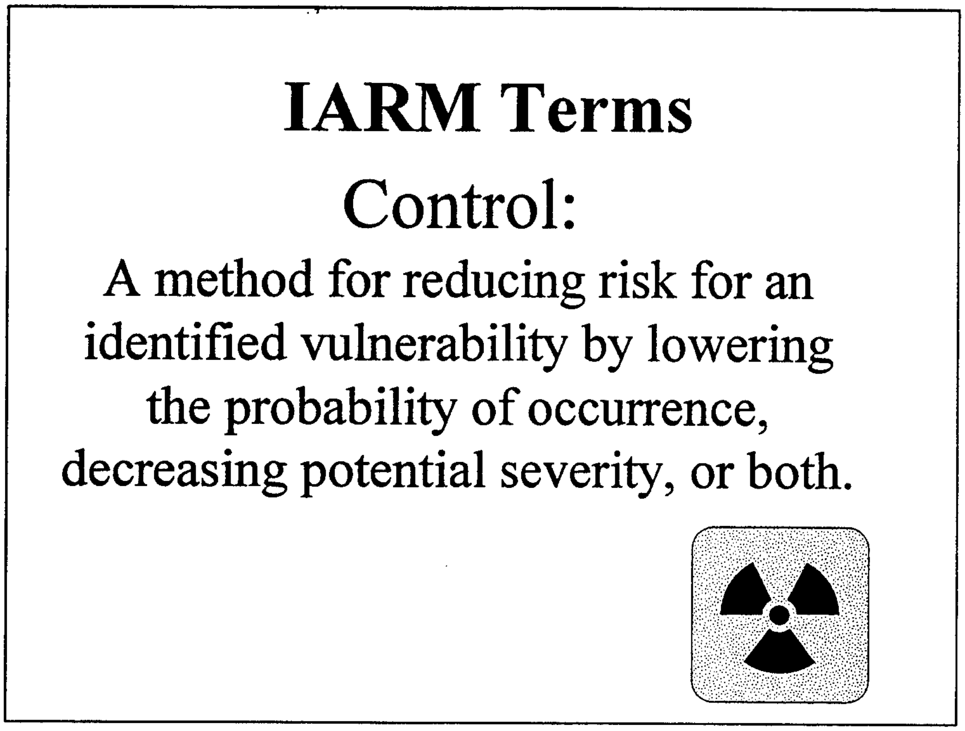
Risk Assessment:

The process of detecting vulnerabilities and assessing associated risks.

<u>Read definition</u>. Risk assessment is the first two steps of the five step risk management process

FIRST:

1. **Identify vulnerabilities**
2. **Assess vulnerabilities**

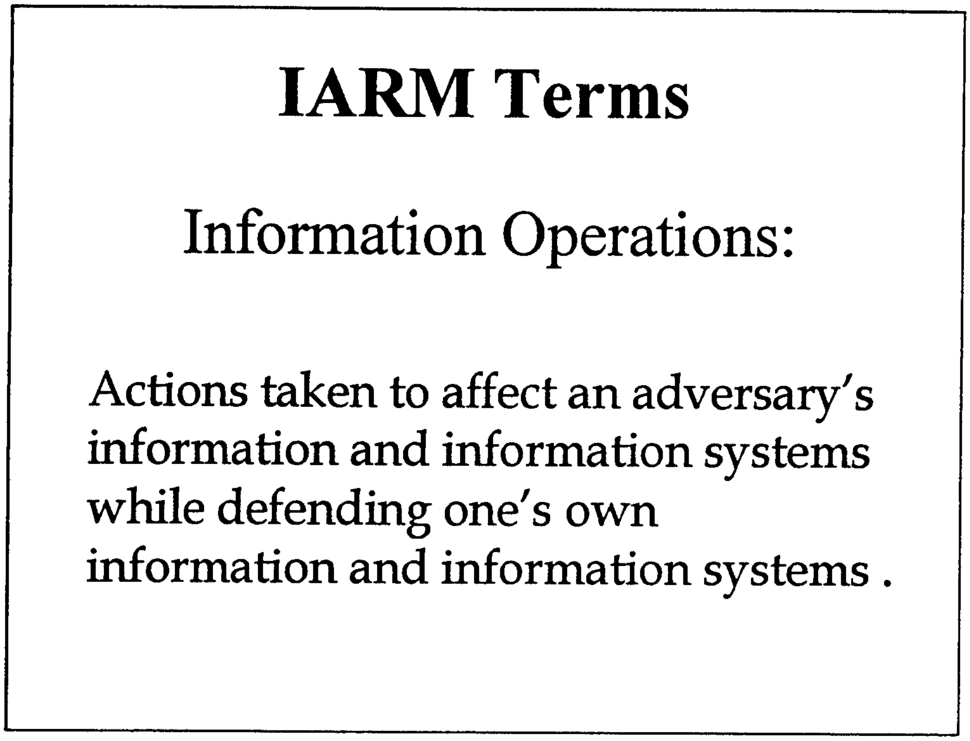


IARM Terms

Control:

A method for reducing risk for an identified vulnerability by lowering the probability of occurrence, decreasing potential severity, or both.

<u>Read definition</u>. RADM Giffin, during his last GW battle group's deployment required his staff to present both types of controls for significant risks when using ORM for their activities. The first would lower the probability of something bad happening; the second would decrease the severity if the event did occur.



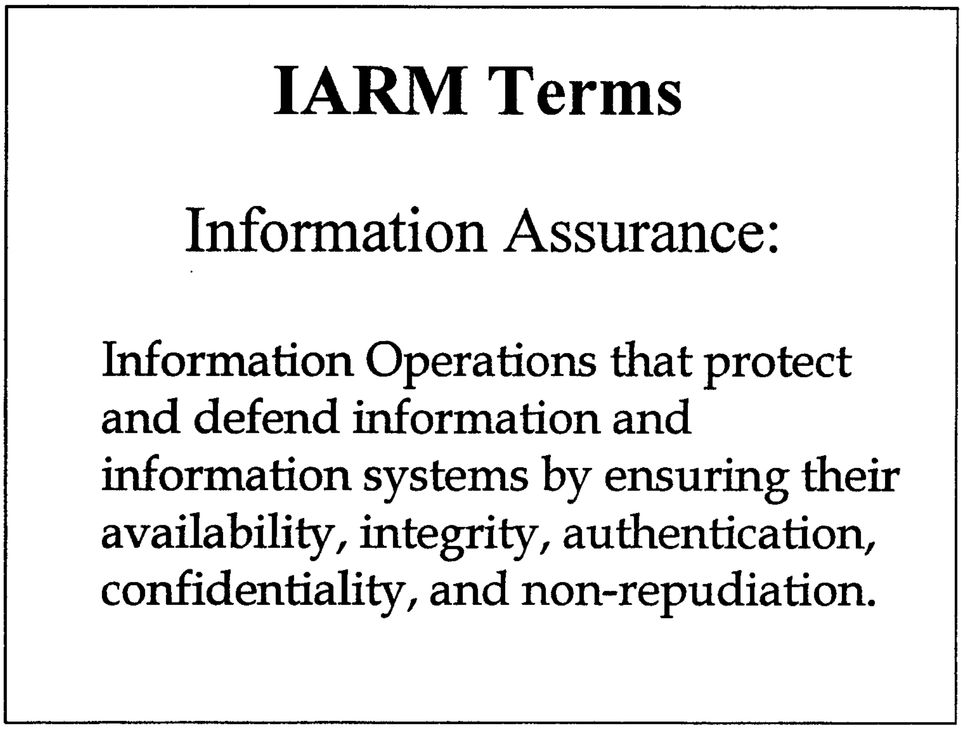
IARM Terms

Information Operations:

Actions taken to affect an adversary's information and information systems while defending one's own information and information systems .

Read Definition. Actions taken to affect an adversary's information and information systems while defending one's own information and information systems.

Note: It may be worthwhile to note that we are not just talking about computers systems, but the whole range of information systems that we rely on to move information around. These systems are becoming more critical in the Navy's move to Network-Centric Warfare and our military's overall Information Operations.

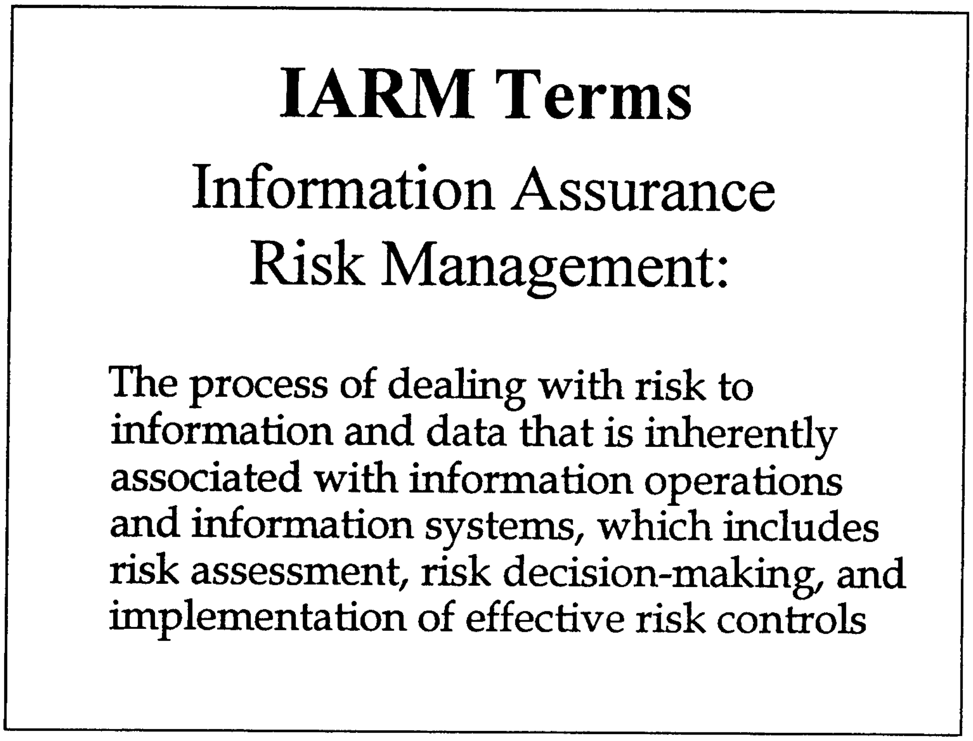


IARM Terms

Information Assurance:

Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Read Definition. Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.



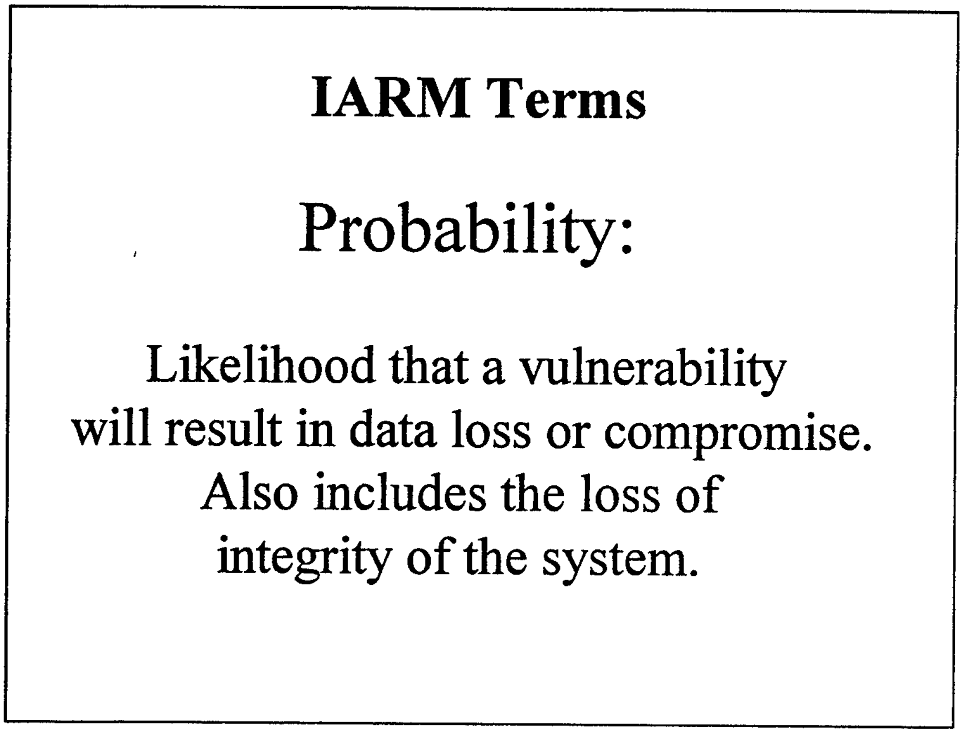
IARM Terms

Information Assurance Risk Management:

The process of dealing with risk to information and data that is inherently associated with information operations and information systems, which includes risk assessment, risk decision-making, and implementation of effective risk controls

Read Definition. The process of dealing with risk to information and data that is inherently associated with information operations and information systems, which includes risk assessment, risk decision-making, and implementation of effective risk controls.

Note: IARM is not just for computer networks, but includes any information system or process!!!

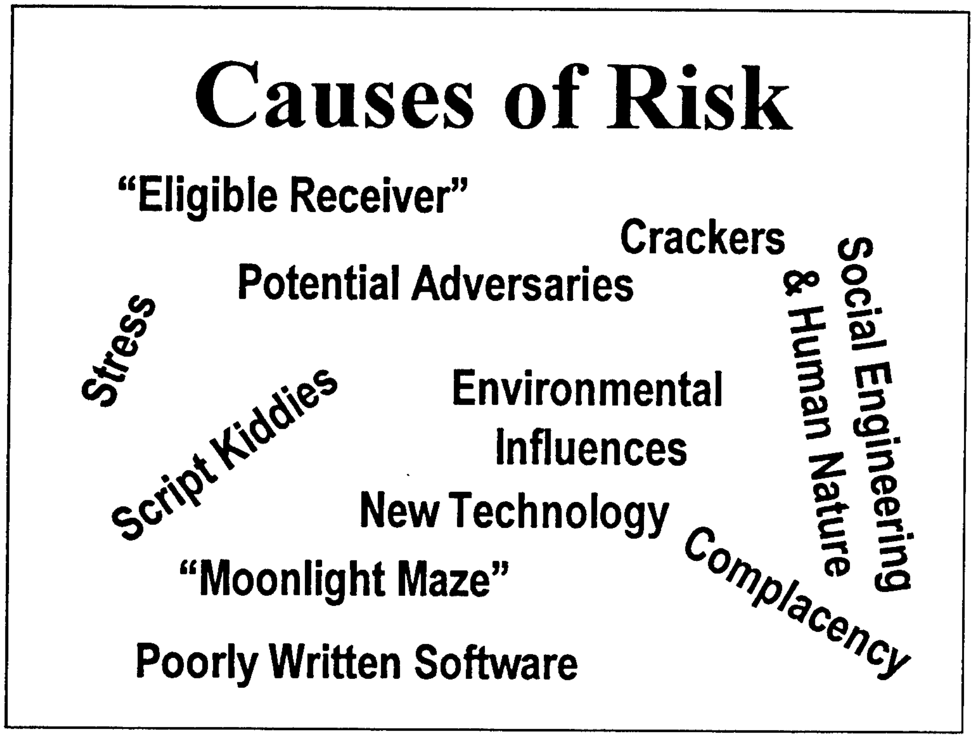


IARM Terms

Probability:

Likelihood that a vulnerability will result in data loss or compromise. Also includes the loss of integrity of the system.

<u>Read definition.</u> The likelihood that a vulnerability will result in data loss or compromise is based on factors such as location, exposure, personnel, experience and historical information.



Causes of Risk

"Eligible Receiver"

Crackers

Social Engineering

& Human Nature

Potential Adversaries

Stress

Script Kiddies

Environmental Influences

New Technology

Complacency

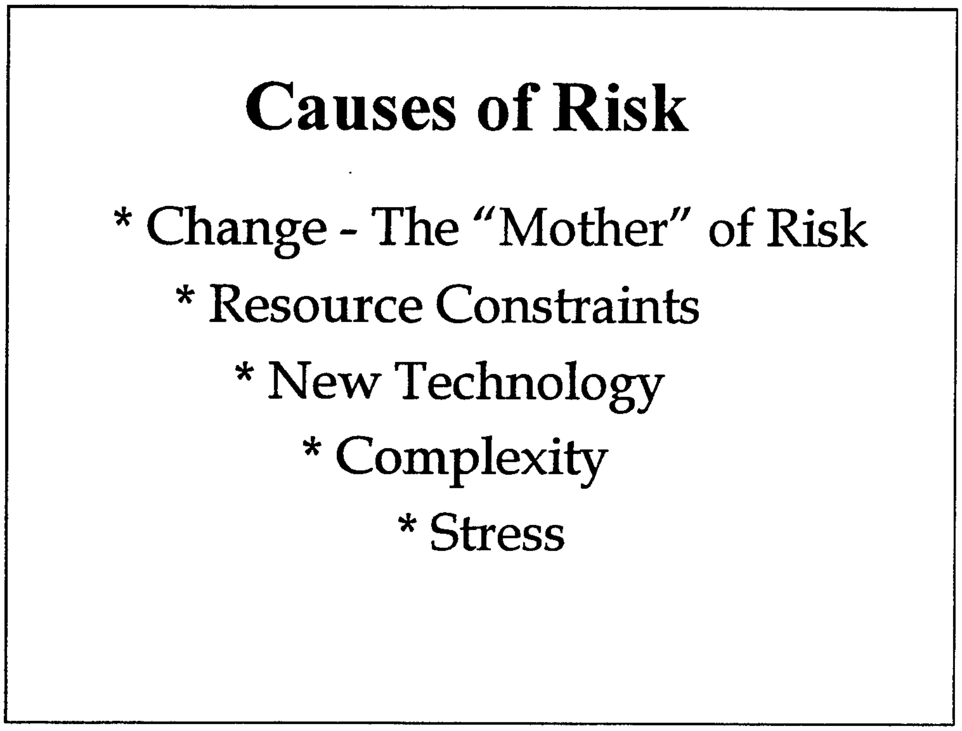
"Moonlight Maze"

Poorly Written Software

The causes of risk to the security of information systems are great and varied. One has only to pick up the newspaper to read about some intrusion of a major commercial or government site.

Point out what Social Engineering is and that the only sure way to protect against it is effective user training.

Certainly the risk that Navy computer networks face are as great as any a fleet unit would face in its normal operating environment!



Causes of Risk

* Change - The "Mother" of Risk

* Resource Constraints

* New Technology

* Complexity

* Stress

These are some of the things we face in the naval service which tend to cause risk. Thses apply to all facets of our daily activity:

- Change is the big one...anything from adding a new user to changing a networks' configuration. Changes should alert us to new hazards and increased risk.

- "Doing more with less" seems to be the motto of the naval service...how long can we keep stretching our resources? What's the risk involved?

- New technology is great, but sometimes the gain from increased capabilities is offset by our human abilities to absorb all the new information or adapt to the new equipment. How much training to maintainers get when we add a new device like a VPN to a network?

- The more complex the problem, usually, the riskier. There are more ways for things to go wrong.

- We see in an analysis of mishap causal factors that human error occurs in 80% of our mishaps. Stress significantly affects the ability of those humans to perform!

Causes of Risk

(Cont.)

* Human Nature

* High Energy Levels

* Societal Constraints

* Environmental Influences

* Speed/Tempo of Operation

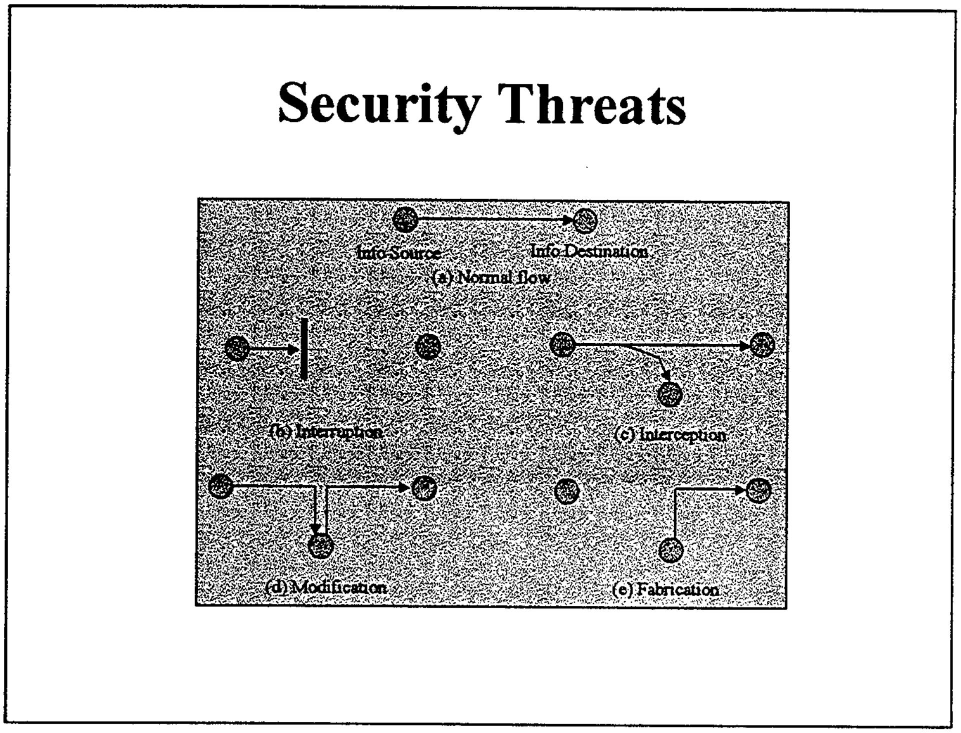
- Humans tend to make mistakes, miscommunicate, have personality conflicts, get fatigued, get complacent and so on. We need to recognize the potential for human nature to present risk in our operations.

- Nervous energy, excitement associated with new situations and perceived pressure to perform can all increase risk (ie, NATOPS check, AC emergency). A recent study of AIRLANT/ AIRPAC mishaps shows that 56% of the deployment mishaps over the past 5 years (FY91 through 1st quarter FY96) occurred during the first two months of deployment.

- Society's standards and expectations drive public opinion, which has an important bearing on our budget and livelihood. So things which negatively affect our command image in the public eye can certainly present risk to our organization (and our careers). Crashing into a school, for example, is simply unacceptable.

-Environment (e.g.. weather, sea state) is always a significant consideration in naval operations.

- Risk certainly increases when the tempo of operations is high. It can also increase when the tempo is low, due to complacency.

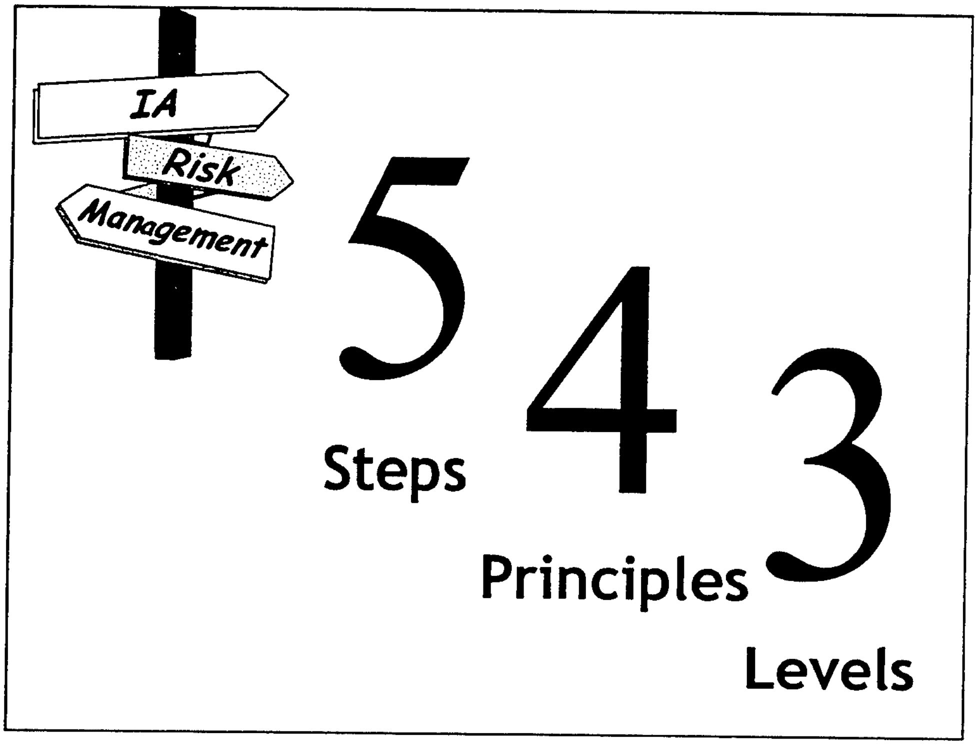


Security Threats

This slide is presented as a review of the threats to the flow of information that information systems are exposed to in a normal operating environment.

A threat is anything that can copy, modify, disrupt, or destroy information and data.

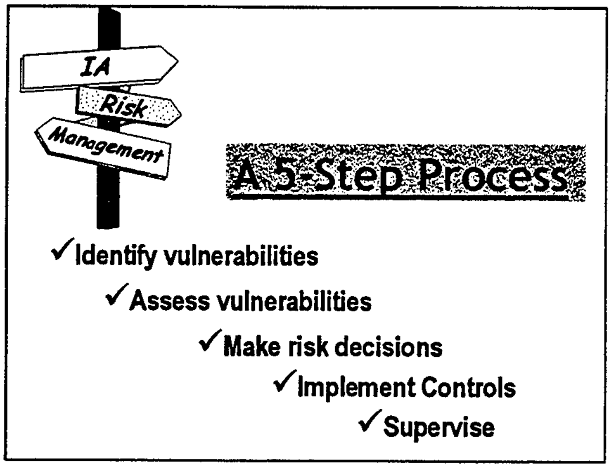
The SANS Institute keeps an ongoing list of the top 10 security vulnerabilities at www.sans.org/topten.html. Obviously, this SANS list applies predominately to computer networks.



5 Steps 4 Principles 3 Levels

Think of IARM as a 5-4-3 process.

5 STEPS
4 PRINCIPLES
3 LEVELS or APPLICATIONS


IA
Risk
Management

A 5-Step Process

✓Identify vulnerabilities

✓Assess vulnerabilities

✓Make risk decisions

✓Implement Controls

✓Supervise

IARM is a simple five-step process. The concept of applying a standard, systematic approach to minimizing risk was originally developed to improve safety in the development of weapons, aircraft, space vehicles and nuclear power. As I mentioned earlier, it has been embraced by many civilian corporations and the Army, and is now being implemented in the Navy, USMC, Air Force and Coast Guard.

Although a risk management process like this has been part of the NAVOSH program for years, it has traditionally been applied primarily to workplace hazards. However, this process is also effective when applied to planning, operations, training and procedures. The five steps are:

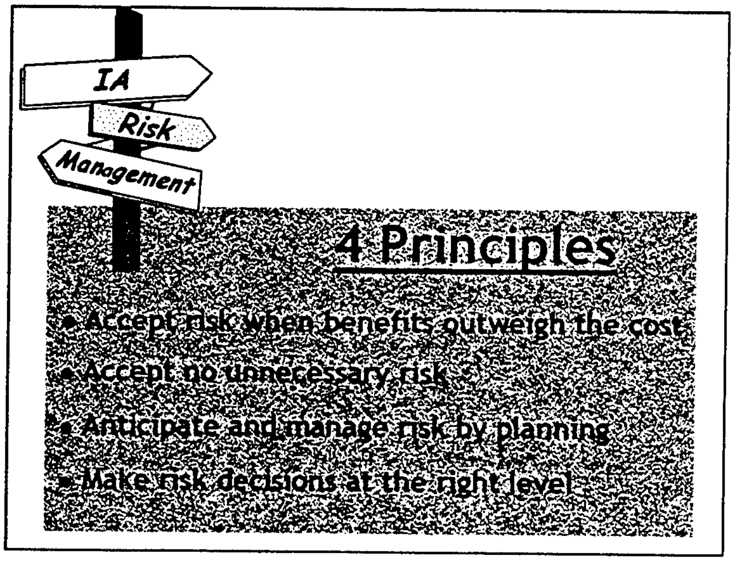
--*Identify vulnerabilities*. Identify potential causes of loss or compromise to information and data, damage to system hardware or mission degradation.

--*Assess vulnerabilities*. For each vulnerability identified, determine the associated risk in terms of severity and probability.

--*Make risk Decisions*. Develop risk control options, then decide if benefit outweighs risk. Seek further controls or guidance from CoC, if necessary.

--*Implement Controls*. Once risk decision is made, implement selected controls.

--*Supervise*. Follow-up to ensure controls are working and watch for changes.


IA
Risk
Management

4 Principles

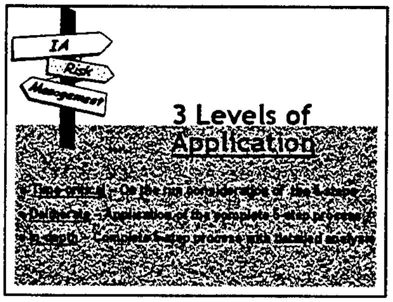
- Accept risk when benefits outweigh the cost
- Accept no unnecessary risk
- Anticipate and manage risk by planning
- Make risk decisions at the right level

1. Risk is inherent in using information systems, and is related to usability. Normally, the greater the usability of a system, the greater the risk.

2. We must take only the risks which are necessary to meet the mission requirements of the system.

3. Risks are more easily controlled when they are identified early in the planning process. This applies to adding new hardware and software, adding new users, or developing new network systems (e.g. NMCI)

4. Normally, this is the leader directly responsible for the network system. However, when that leader determines that the risk is too high, or goes beyond the commander's stated intent, he should seek additional guidance from the chain of command.


IA
Risk
Management

3 Levels of Application

- Time-critical – On the run consideration of the 5-steps
- Deliberate – Application of the complete 5-step process
- In-depth – Complete 5-step process with detailed analysis

The amount of time and level of detail involved in the five steps varies, depending upon the circumstances.

Time-critical IARM entails a quick, mental review or discussion using the five steps during the execution phase of operations/training and for crisis response planning.

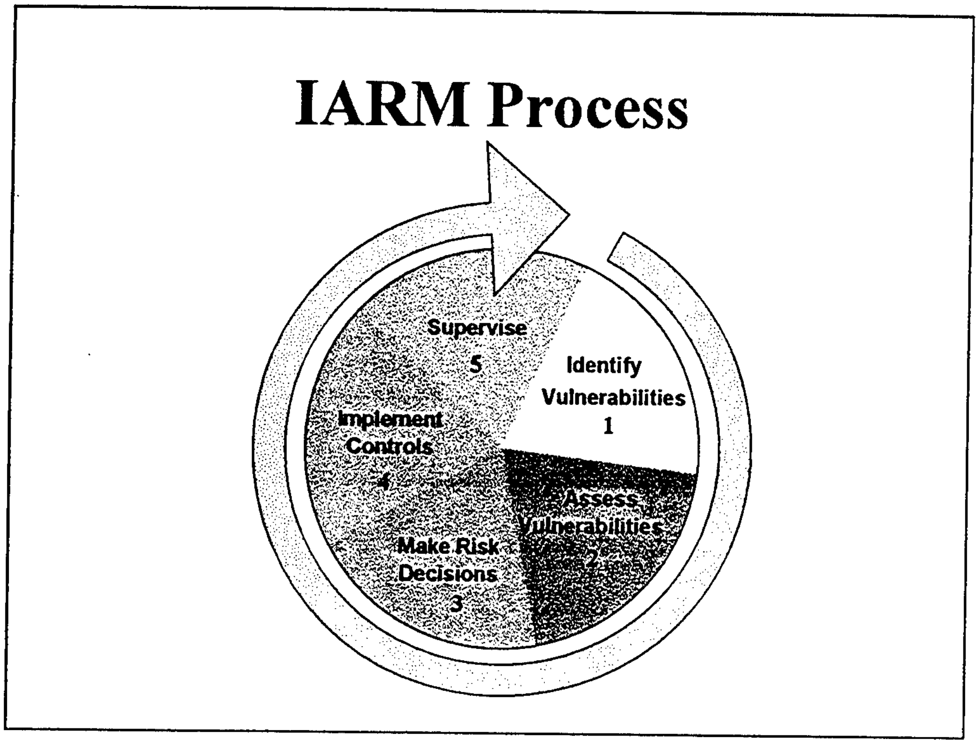
Example of Time-critical IARM: Suspicious Content on a workstation

Deliberate IARM is a slightly expanded, more detailed application of the five steps in planning for an operation or reviewing procedures. This process level is used when there is a good understanding of the vulnerabilities based on experience.

Example of Deliberate IARM: Pre or inter configuration planning (i.e., before and between accreditations possibly).

In-depth IARM is basically the same as deliberate, but with a more thorough risk assessment (first two steps). It is used to more thoroughly explore the vulnerabilities and their associated risk in a complex operation or system, or one in which the vulnerabilities are not well understood.

Example of In-depth IARM: Employment of a new network system



IARM Process

Identify Vulnerabilities 1

Assess Vulnerabilities 2

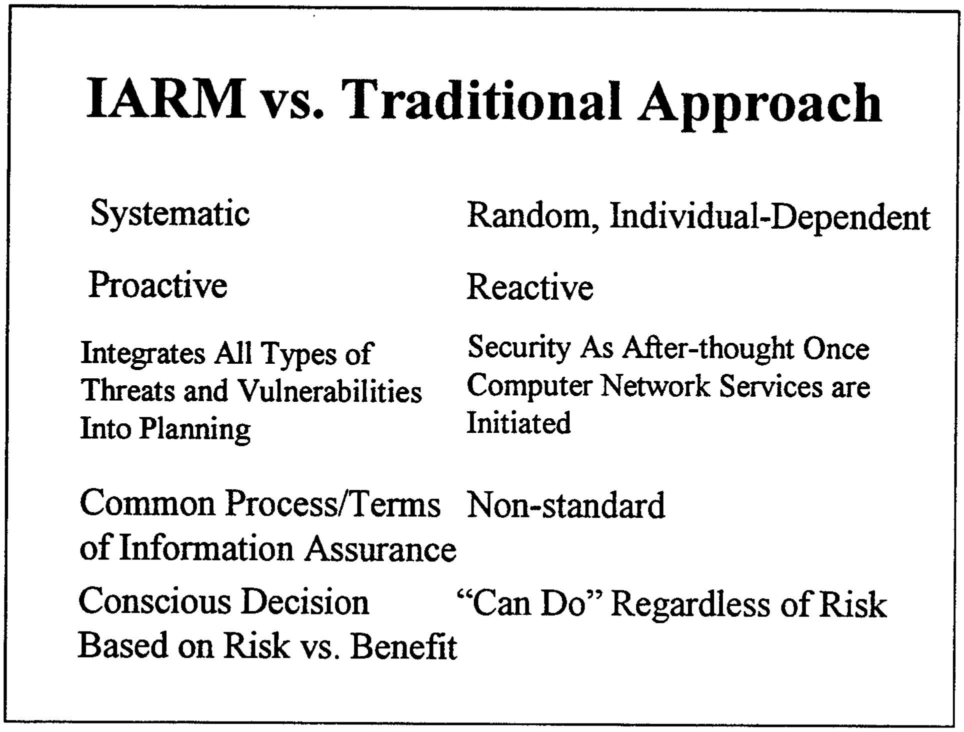
Make Risk Decisions 3

Implement Controls 4

Supervise 5

To summarize, we've depicted the 5 steps of IARM in a pie diagram to help you visualize the continuous nature of the IARM process.

4



IARM vs. Traditional Approach

Systematic	Random, Individual-Dependent
Proactive	Reactive
Integrates All Types of Threats and Vulnerabilities Into Planning	Security As After-thought Once Computer Network Services are Initiated
Common Process/Terms of Information Assurance	Non-standard
Conscious Decision Based on Risk vs. Benefit	"Can Do" Regardless of Risk

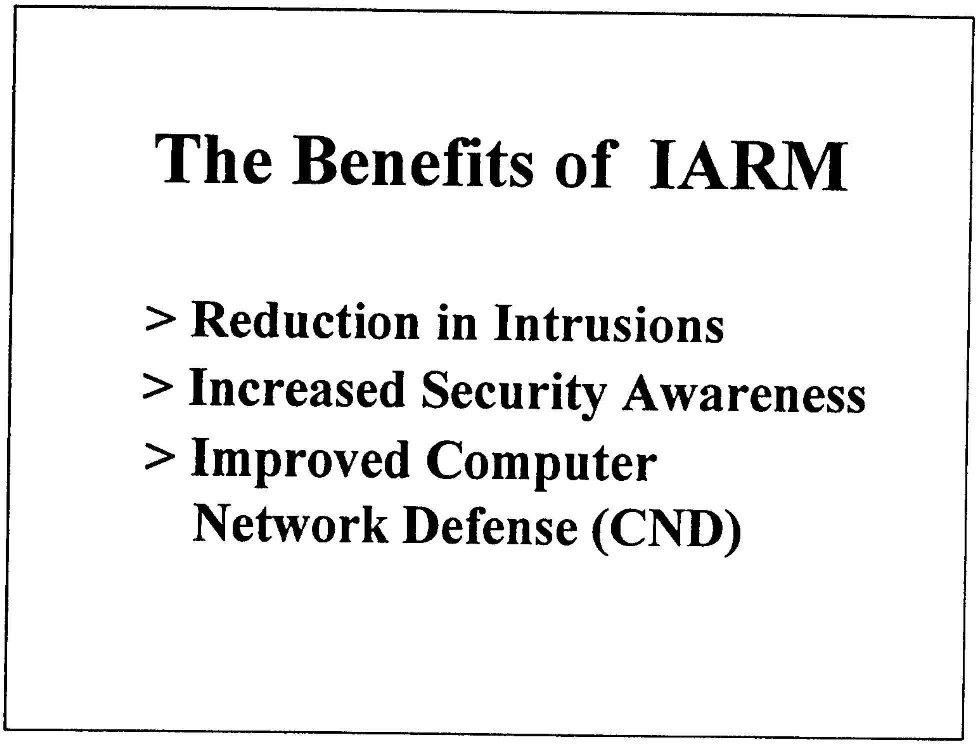
Although the five steps of IARM are a lot like the decision-making process that good, security-knowledgeable system administrators would always used, applying a standard process is different in some important ways.

- IARM is more systematic. Frequently, threat identification and vulnerability assessment is random, and highly dependent upon an individual's past experience and computer network skills. IARM requires users, system administrators and decision makers to focus on threat at a time, shoring up that vulnerability before moving on to the next.

- IARM is more proactive. It requires an attempt to identify ALL threats and potential exploits, not just the ones that have occurred on that computer network in the past.

- IARM addresses all types of threats and vulnerabilities that could threaten our ability to keep network security services unimpaired (social engineering, virus detection, configuration management, user awareness, fiscal limitations, credibility, physical security, computer equipment failures, etc.) This allows effective prioritization of computer network related risks, which helps focus limited time/assets on the most important issues, rather than addressing security threats as an after-thought, once the policies have been formulated or computer network systems created.

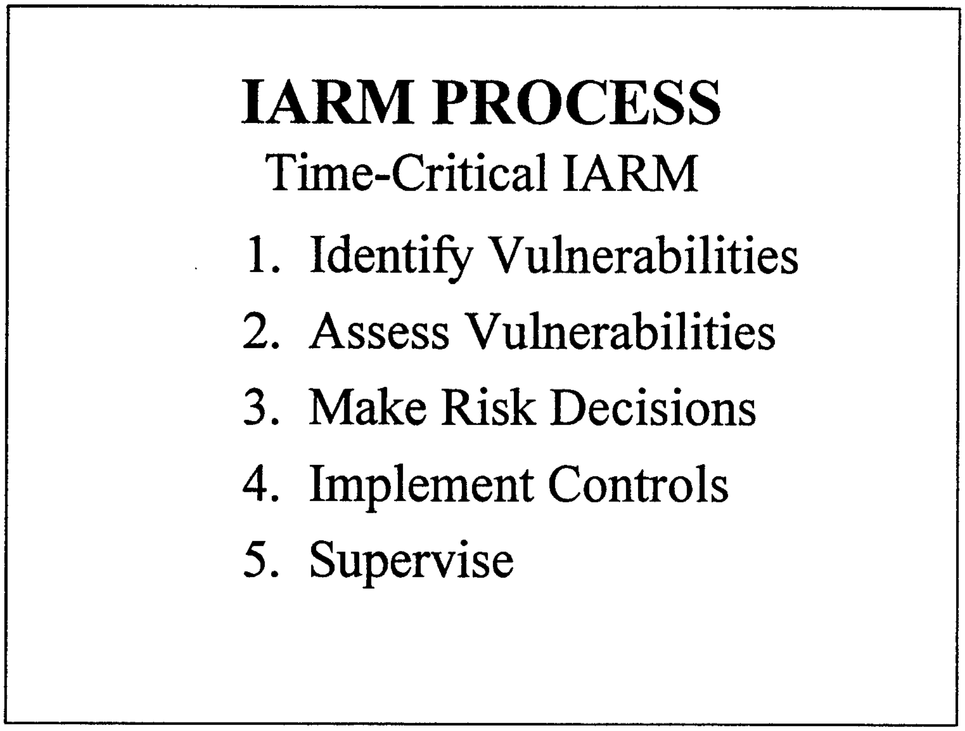
- IARM enhances communication about threats and vulnerabilities by providing a common process and set of terms. It provides a means to articulate concerns and justify decisions to those who may not be completely aware or knowledgeable on the risks entailed in using computer networks.



The Benefits of IARM

> Reduction in Intrusions
> Increased Security Awareness
> Improved Computer
Network Defense (CND)

Though IARM, and risk management in general, is not very precise, it does offer benefits which can enhance a computer network system's defensive performance, in addition to those benefits listed above. It improves general security and information assurance awareness among users, IT support personnel and decision makers. Discussing issues of security can raise the general level of interest and concern. IT support personnel and decision makers may now have a comprehensive list of assets and vulnerabilities associated with those assets where none existed before. Decision makers now have an improved basis for implementing controls, justifying those controls which may prove inconvenient or expensive, and continuing the search for more effective controls should the need arise. Finally, IARM is a continuous, non-static process that can be applied by users, IT support personnel and decision makers alike, giving the whole chain of command the opportunity to personally make a positive contribution to DON's computer network defense performance and overall information systems security.



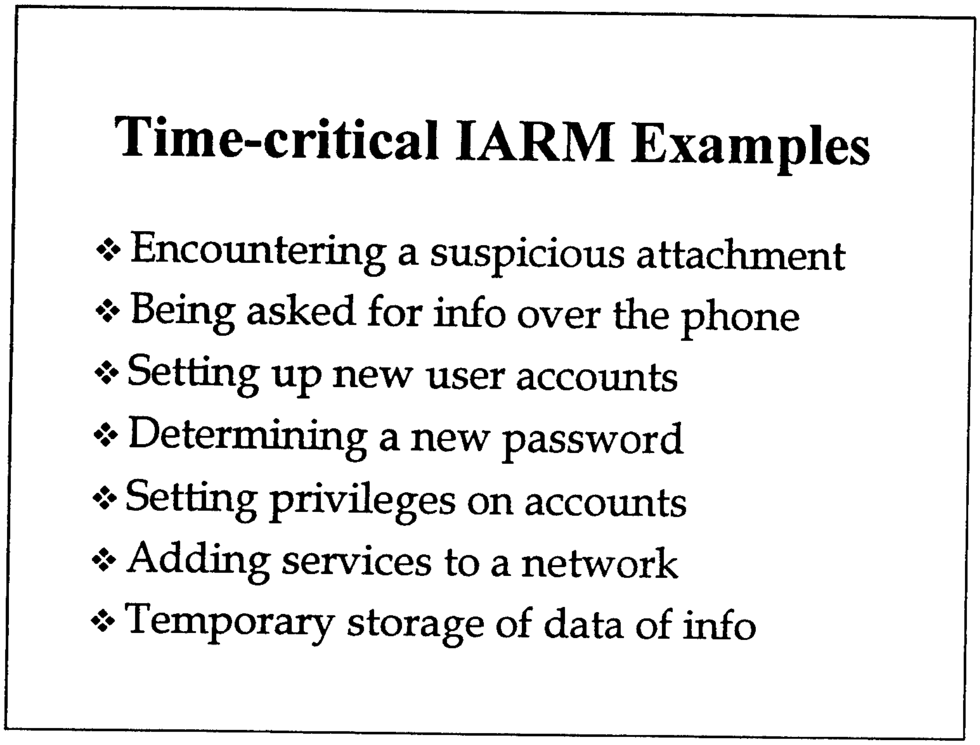
IARM PROCESS

Time-Critical IARM

1. Identify Vulnerabilities
2. Assess Vulnerabilities
3. Make Risk Decisions
4. Implement Controls
5. Supervise

Let's talk about the time-critical IARM process. This is IARM on the most basic level, and is used during execution of ops/training or short-fused planning. Most of you probably use it instinctively without recognizing it as a formal process. However, the more deliberate and in-depth IARM you have done, the more systematic and thorough your time-critical IARM will become.

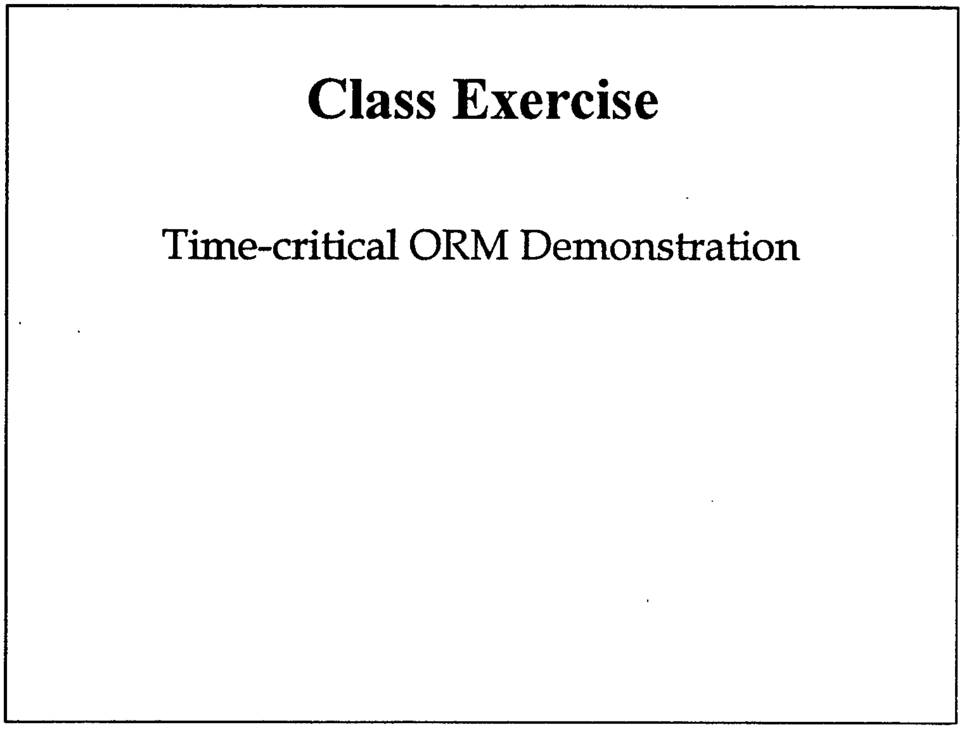
1. Visualize the expected flow of events and identify any conditions which might result in data or information loss or compromise, hardware damage or degraded system performance. If some prior planning has been done, focus on changes in the operation/activity from the original plan.
2. Determine which of the identified vulnerabilities present the greatest risk, considering the potential outcomes and their probability.
3. Determine what controls can be implemented to counter the highest-risk vulnerabilities and what course of action will best accomplish the mission/tasks with an acceptable level of risk. Ensure benefits of the selected course of action outweigh the risk.
4. Implement the controls and the course of action decided on in step three.
5. Monitor the operation/activities for effectiveness of controls and changes. Correct ineffective controls and begin the IARM process again as further changes occur.



Time-critical IARM Examples

- Encountering a suspicious attachment
- Being asked for info over the phone
- Setting up new user accounts
- Determining a new password
- Setting privileges on accounts
- Adding services to a network
- Temporary storage of data of info

Here are some examples of where time-critical IARM could be used.



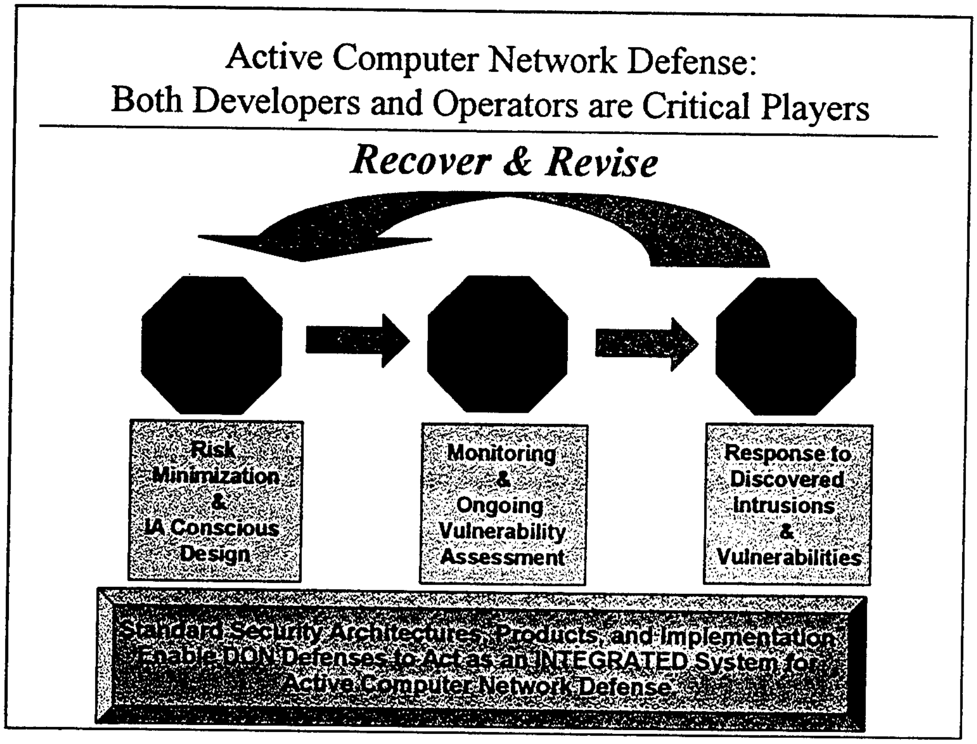
Class Exercise

Time-critical ORM Demonstration

Let's try this time-critical IARM process together. Here's the scenario:

You can use one of the examples from the previous slide

(Turn off projector, hand out example scenario and guide class through 5 steps, writing their responses on the board.)



Active Computer Network Defense:
Both Developers and Operators are Critical Players

Recover & Revise

Risk Minimization & IA Conscious Design

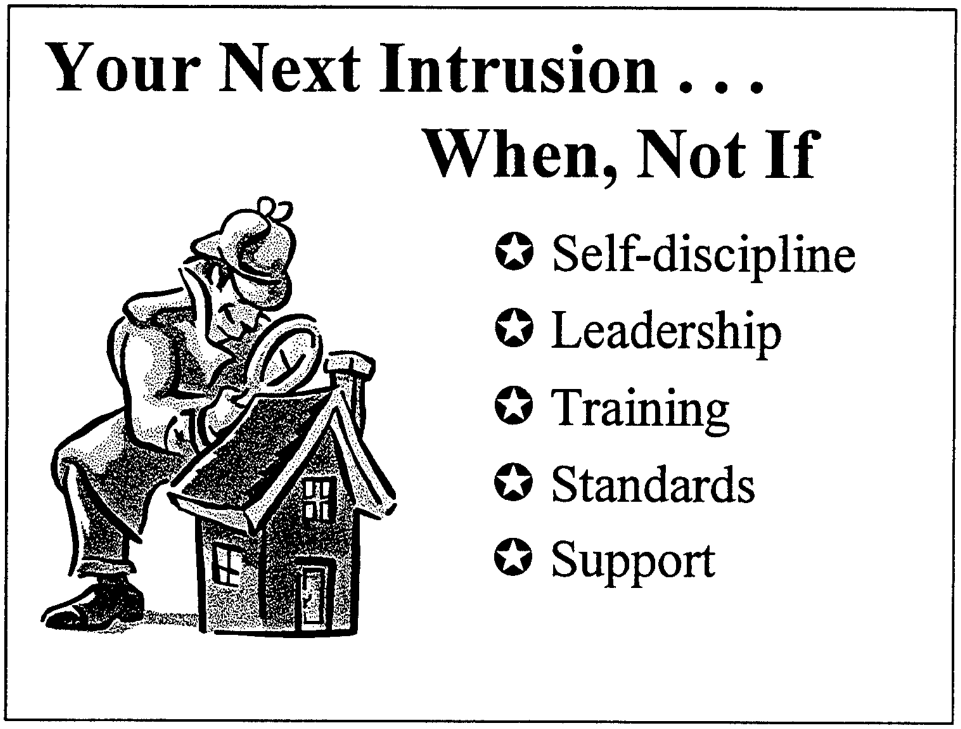
Monitoring & Ongoing Vulnerability Assessment

Response to Discovered Intrusions & Vulnerabilities

Standard Security Architectures, Products, and Implementation Enable DON Defenses to Act as an INTEGRATED System for Active Computer Network Defense

This slide is from SPAWAR for the NMCI concept of operations for security. Notice how it resemble some of the aspects of IARM.

Note: IARM assumes more of a systems approach and can be used at the user level all the way up to the senior decision makers.



Your Next Intrusion . . .

When, Not If

✪ Self-discipline

✪ Leadership

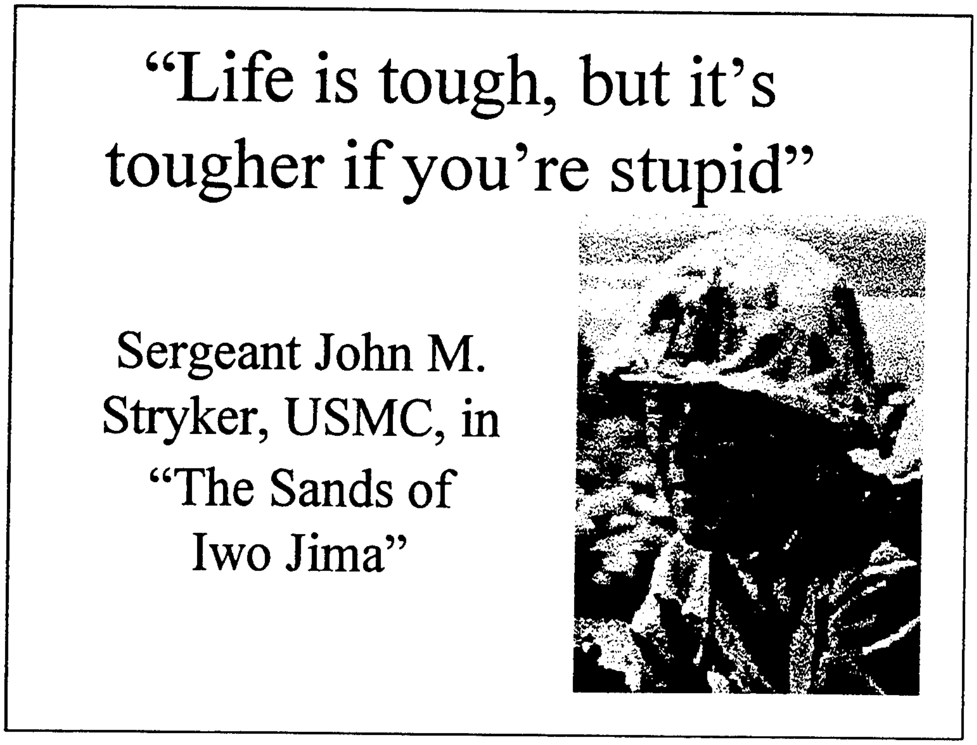
✪ Training

✪ Standards

✪ Support

Our next intrusion mishap is when, not if. The human will fail in one of the 5 areas listed. It is leadership's challenge to ensure processes are in place to detect the deviation before it leads to an intrusion and security lapse in the network system.

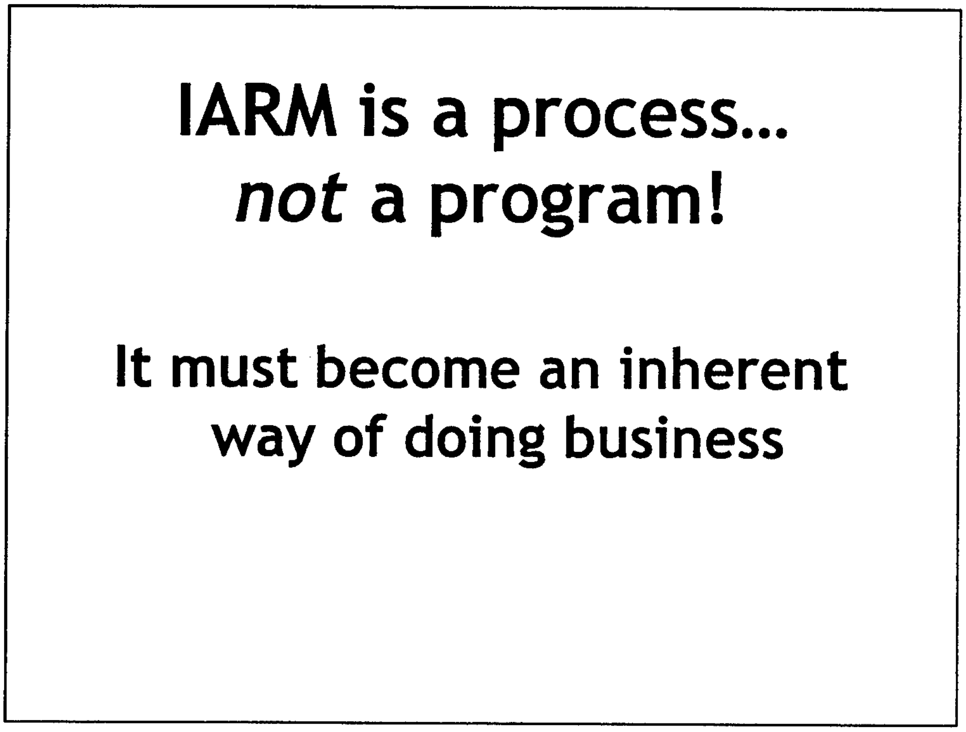
Self-discipline
Leadership
Training
Standards
Support



“Life is tough, but it’s tougher if you’re stupid”

Sergeant John M. Stryker, USMC, in “The Sands of Iwo Jima”

This quote is illustrative of many attitudes towards IA. Its going to remain a difficult task if the folks who interact with our computer networks don’t get smart. IARM is a means by which we can all get smart and improve overall CND in the Navy.



IARM is a process…
not a program!

It must become an inherent way of doing business

Thanks for your attention...

Think IA!

LIST OF REFERENCES

Chief of Naval Operations, OPNAVINST 3500.39, "Operational Risk Management (ORM)," 03 April 1997.

Chief of Naval Operations, OPNAVINST 5239.1B, "Navy Information Assurance (IA) Program," 09 November 1999.

Critical Infrastructure Assurance Office (CIAO), "Practices for Securing Critical Information Assets," [http:www.ciao.gov]. January 2000.

Denning, Dorothy E., "Information Warfare and Security," Addison-Wesley, 1999.

Jackson, William, "Top 10 System Security Threats are Familiar Foes," *Government Computing News*, vol.6, no. 8, August 2000. [http://www.gcn.com/stste/vol6_no8/news/812-1.html]

Pfleeger, Charles D., "Security in Computing," 2nd ed., Prentice Hall PTR, 1997.

SANS Institute, "Security Essentials Certification 1," by Green, John, SANS Sixth Annual Conference on Securing Networks and Systems, 20 October 2000.

SANS Institute, "Security Essentials Certification 2," by Cole, Eric, SANS Sixth Annual Conference on Securing Networks and Systems, 21 October 2000.

Scambray, J., McClure, S., Kurtz, G., "Hacking Exposed: Network Security Secrets and Solutions," 2nd ed., McGraw-Hill, 2001.

Stallings, William, "Network Security Essentials: Applications and Standards," Prentice Hall, Inc., 2000.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Brenton, Chris, "Mastering Network Security," SYBEX, Network Press, 1999.

Center for Strategic and International Studies, "Cyber Threats and Information Security: Meeting the 21st Century Challenge," by Borchgrave, A., and others, December 2000.

CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, "Results of the Distributed-Systems Intruder Tools Workshop: November 2-4, 1999," 7 December 1999.

U.S. General Accounting Office, Account and Information Management Division, "GAO/AIMD-98-68 Information Security Management," May1998.

U.S. General Accounting Office, Account and Information Management Division, "GAO/AIMD-99-139 Information Security Risk Assessment," August 1999. (Exposure Draft)

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center.. 2
8725 John J. Kingman Road, STE 0944
Fort Belvoir, VA 22060-6218

2. Dudley Knox Library.. 2
Naval Postgraduate School
411 Dyer Road
Monterey, CA 93943-5101

3. LCDR Ernest D. Hernandez... 2
1121 David Ave
Pacific Grove, CA 93950-5417

4. Professor Daniel Warren, Code CS/Wd 1
Naval Postgraduate School
Monterey, CA 93943-5118

5. Professor Rex Buddenberg, Code IS/Bu.. 1
Naval Postgraduate School
Monterey, CA 93943-5118

6. Commanding Officer.. 1
Fleet Information Warfare Center
2555 Amphibious Drive
Norfolk, VA 23521-3225

7. Chair, IS Academic Group, Code IS 1
Naval Postgraduate School
Monterey, CA 93943-5118

8. The School of Aviation Safety 1
Naval Postgraduate School (Code 10)
1588 Cunningham RD, RM 301
Monterey, CA 93943-5202

9. Center for Executive Education 1
Code 01E
Naval Postgraduate School
555Dyer Road
Monterey, CA 93943-5118

10. DON CIO 1
1000 Navy Pentagon
Washington, DC 20350-1000

11. Commandant (G-OC) 1
US Coast Guard
Washington, DC 20593

12. Commander Naval Security Group (N7) 1
9800 Savage Road, Suite 6585
Fort Meade, MD 20755-6585

13. Commandant of the Marine Corps (Code C4) 1
Headquarters Marine Corps
2 Navy Annex
Washington, DC 20380-1775

14. US Pacific Command (USPACOM) 1
Attn: J39
Box 64013
Camp H.M. Smith, HI 96861-4013

15. Office of the CNO (N643) 1
2000 Navy Pentagon
Washington, DC 20350-2000

16. National Infrastructure Protection Center 1
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

17. DISA Headquarters Bldg. 12 1
ATTN: JTF-CND
701 South Courthouse Road
Arlington, VA 22204

18. National Security Agency 1
ATTN: Dr. L. Merritt - IOTC
9800 Savage Road
Ft. George G. Meade, MD
20755-6752